



CERT+ Automation Workflows User Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

Copyright © 2022 AppViewX, Inc. All Rights Reserved.

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

Trademarks

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

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).

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

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface.....	6
Revision History.....	6
About this Guide.....	6
Audience.....	6
Text Conventions.....	6
Chapter 1. Prerequisites	7
Chapter 2. Role-Based Access Control.....	8
Chapter 3. Accessing CERT+ Automation Workflows.....	9
Chapter 4. Accessing CERT Automation Workflow Tasks	13
Chapter 5. Certificate Expiry Workflows.....	18
Overview.....	18
Certificate Expiry Notification based on Certificate Attributes.....	18
Certificate Expiry Notification - Cert Group Hierarchy.....	23
Certificate Expiry Notification - Days.....	28
Certificate Expiry Notification - Devices Servers.....	32
Certificate Expiry Notification.....	38
Update Certificate Attributes.....	42
Certificate Expiry Notification with JIRA.....	47
Certificate Expiry Notification with ServiceNow.....	52
Orphan Certificates Report.....	56
Chapter 6. Create Certificate Workflows.....	62
Overview.....	62
Enroll Certificate and Download.....	62
Certificate Provisioning with Notification.....	72
Enroll Certificate Based on Policy CSR Details CSR Upload.....	82
Manual.....	87
Policy Based.....	93

Upload CSR.....	99
Create LTM SSL Profile and Enroll Certificate.....	104
Manual.....	108
Policy Based.....	118
Upload CSR.....	126
Enroll Certificate with Certificate Group and CSR Upload.....	134
Enroll Certificate With ServiceNow.....	138
Enroll Certificate and Push with ServiceNow.....	149
Easy Certificate Provisioning.....	163
Enroll Certificate with CAA Validation.....	170
Enroll Certificate and Push	181
Manual.....	185
Policy Based.....	194
Upload CSR.....	202
Chapter 7. Renew Certificate Workflows.....	209
Overview.....	209
Renew Certificate.....	209
Regenerate Certificate with New CSR.....	218
Manual.....	221
Upload CSR.....	229
Renew Certificate and Push.....	233
Renew Certificate with ServiceNow.....	246
Renew Certificate and Push with ServiceNow.....	255
Chapter 8. Automation Workflow Tasks.....	265
Overview.....	265
Expiry Task.....	265
Enrollment Tasks.....	276
Renew Tasks.....	288
Renew Task.....	288

Regenerate Task.....	300
Push Tasks.....	312
Chapter 9. Designing a Custom Workflow using OOB Tasks.....	324
Chapter 10. Scheduling an OOB workflow.....	337
Chapter 11. Customizing an OOB Workflow.....	338

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	Indicates commands within a paragraph, URLs, code in examples, text that appears 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

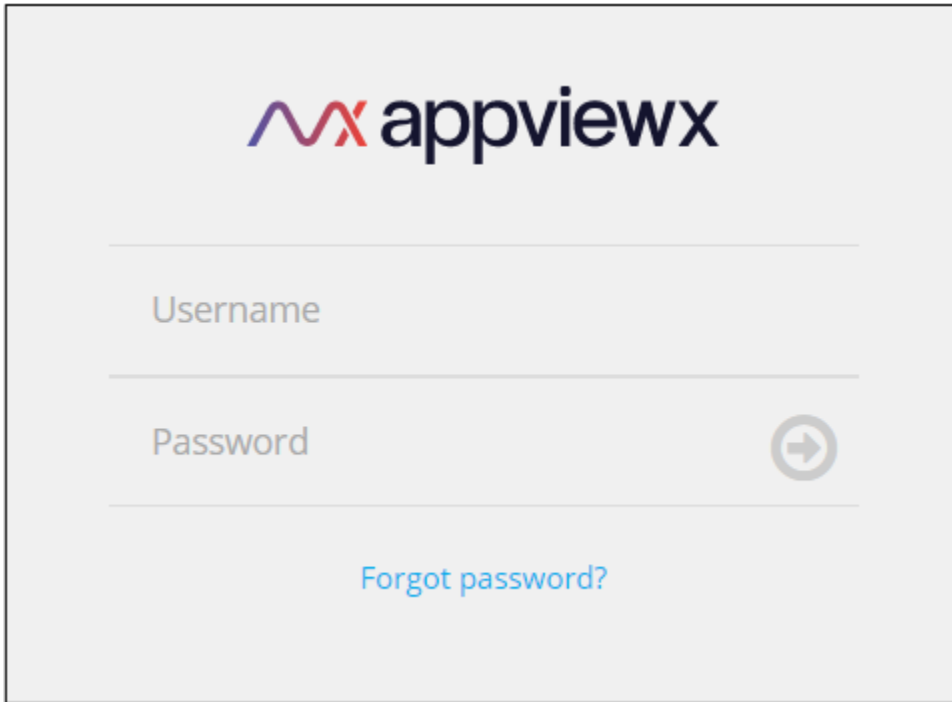
With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to [this link](#) and find out more about RBAC.


Chapter 3: Accessing CERT+ Automation Workflows

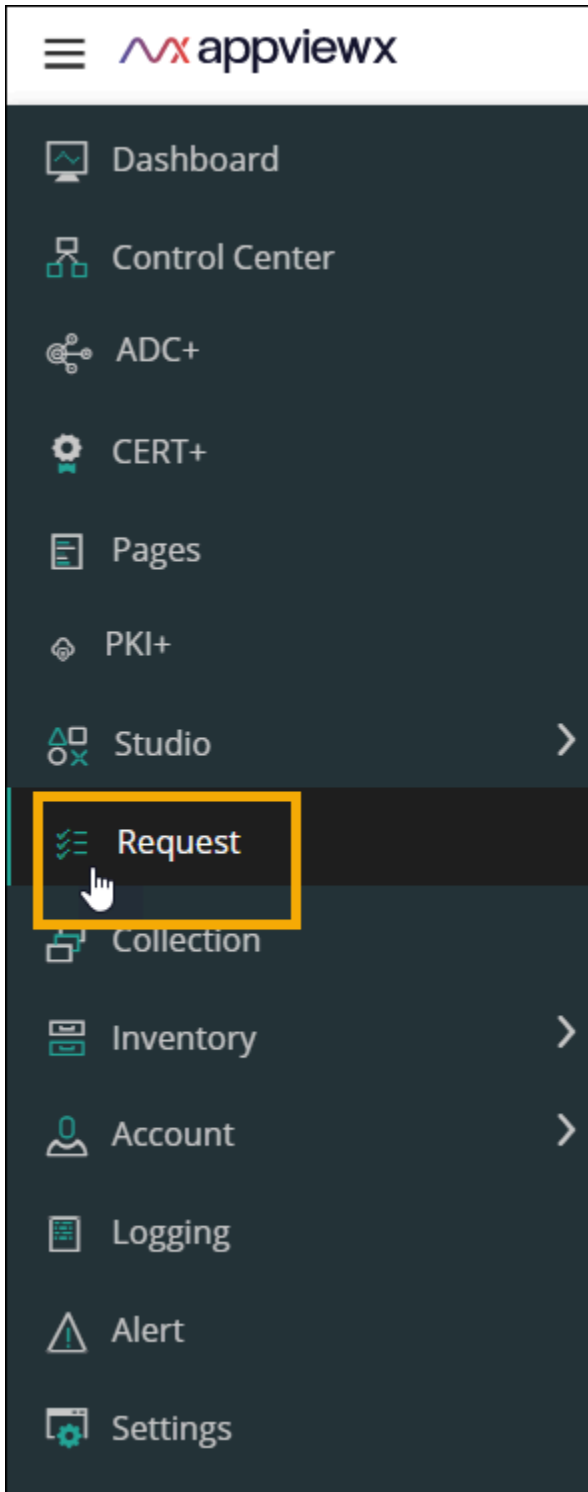
The CERT+ Automation workflows are available on the Workflow **Catalog** page.

To view these workflows:

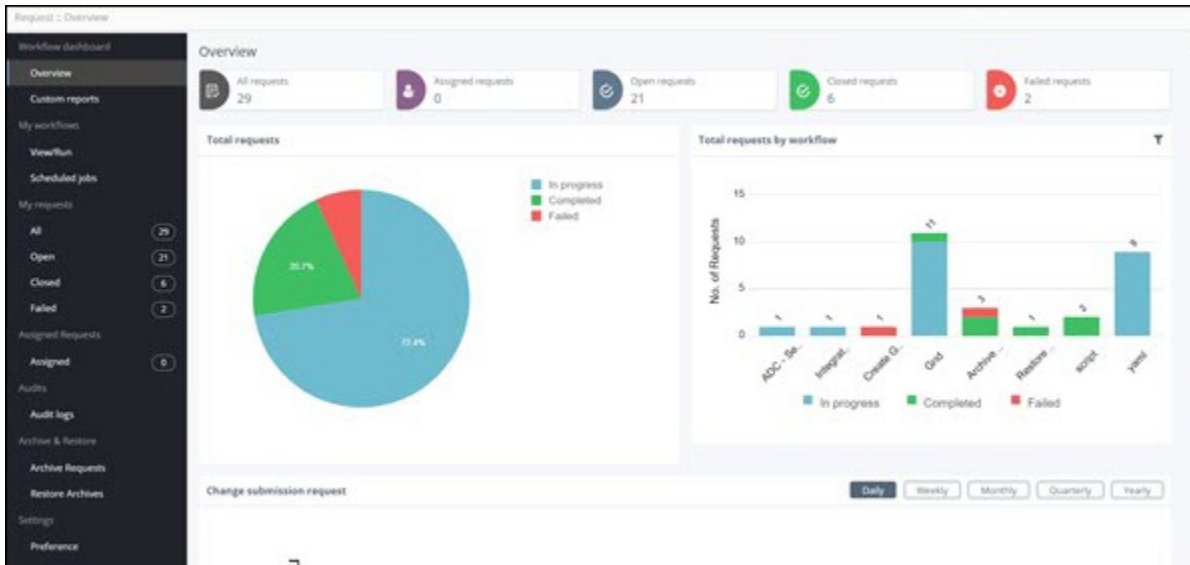
1. Log into AppViewX with valid credentials.

A screenshot of the AppViewX login interface. At the top center is the AppViewX logo, which consists of a stylized 'VX' in red and blue followed by the text 'appviewx' in a dark blue sans-serif font. Below the logo are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. To the right of the password field is a circular icon containing a right-pointing arrow. Below the password field is a blue link that says 'Forgot password?'.

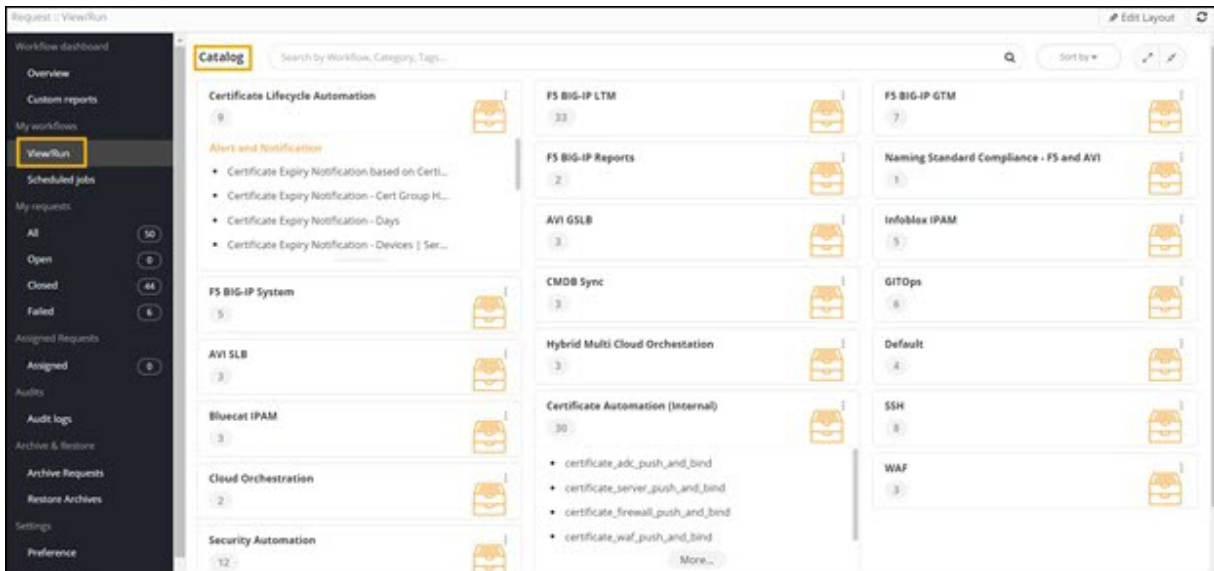
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Request**.



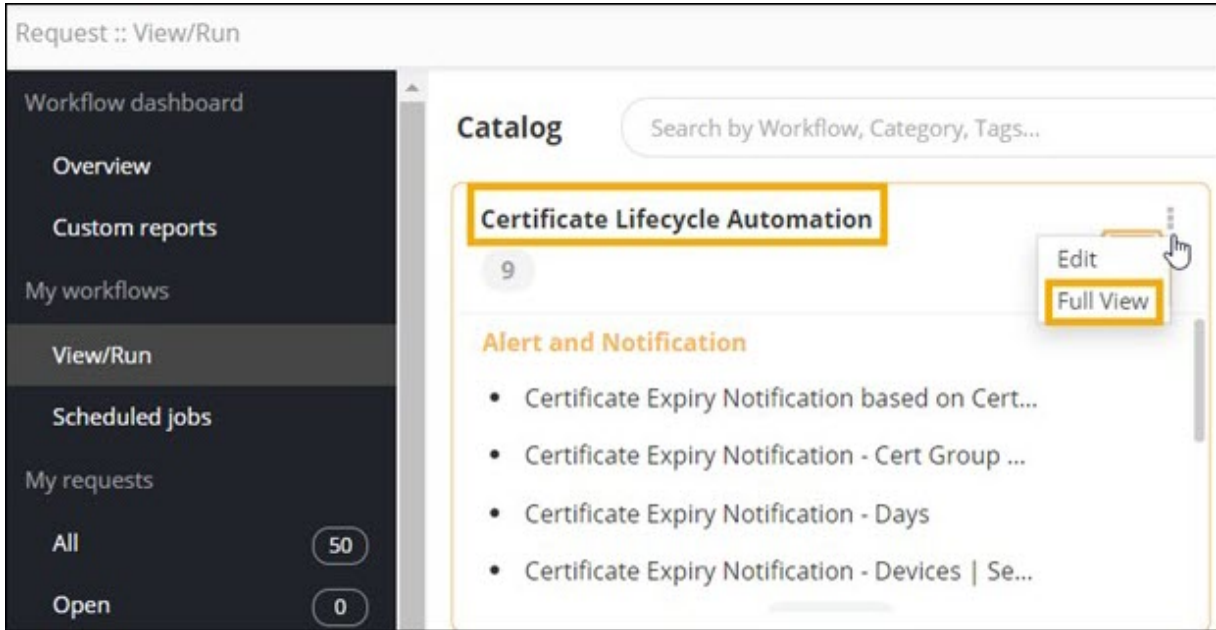
The Workflow **Request** page is displayed, with the **Overview** section open by default.



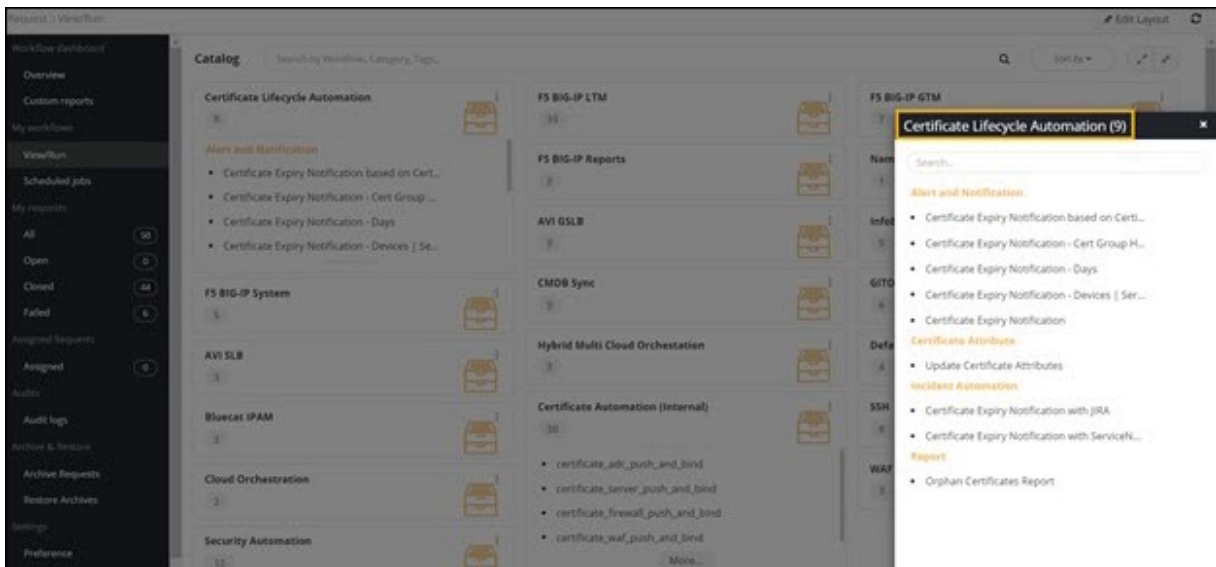
- On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**. The workflow **Catalog** page is displayed.



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



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

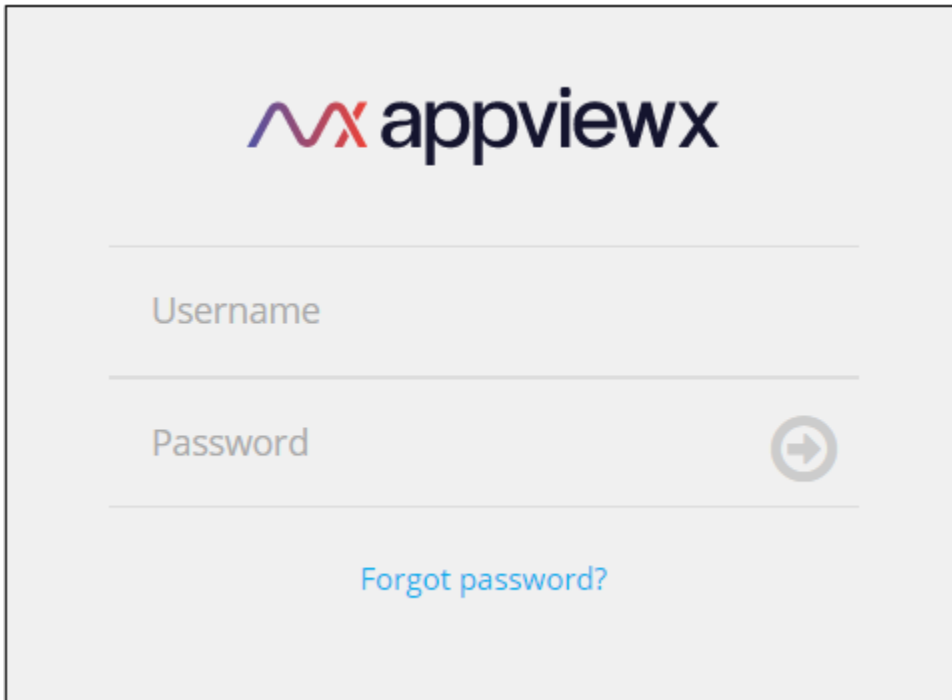



Tip: You can also search for a workflow on the **Catalog** page by typing the keyword(s) in the search bar.

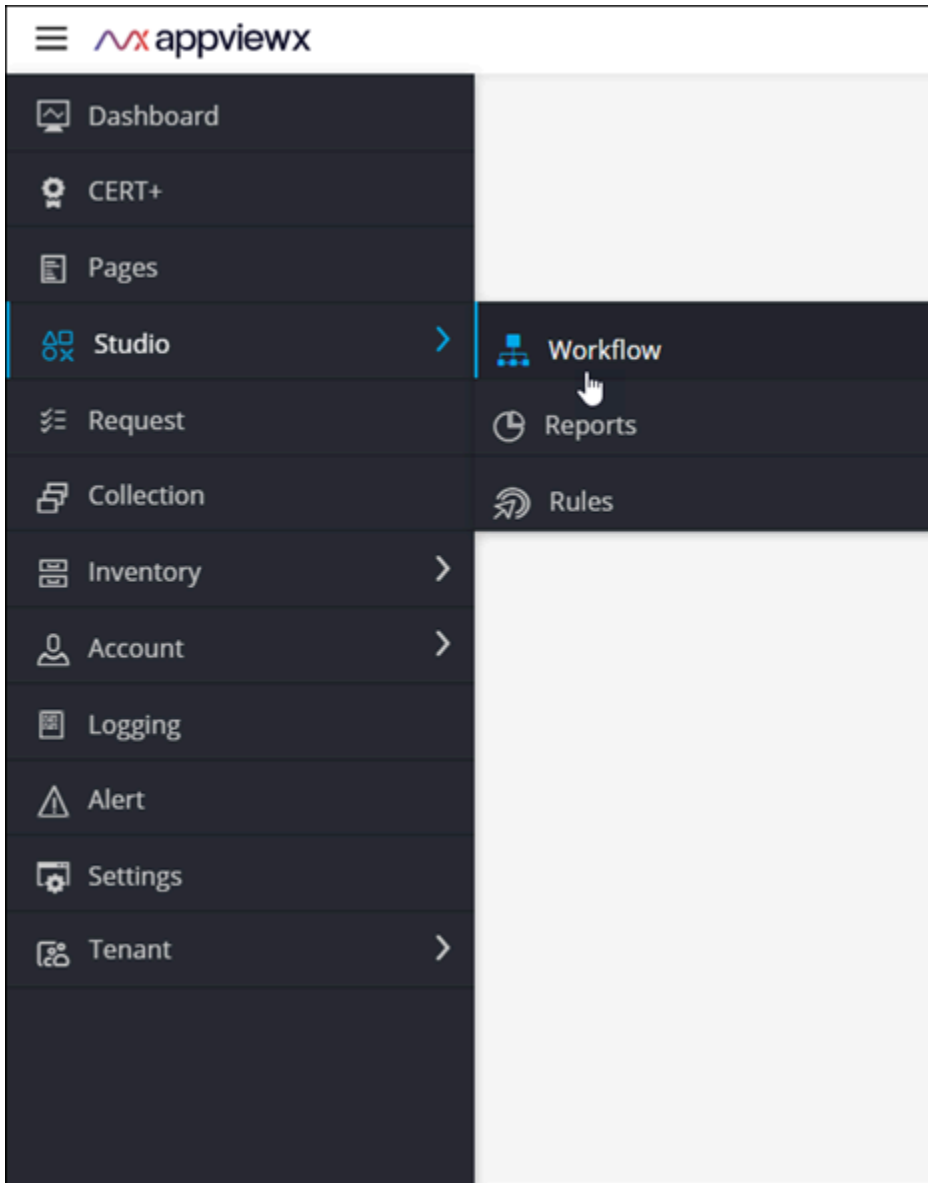
Chapter 4: Accessing CERT Automation Workflow Tasks

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

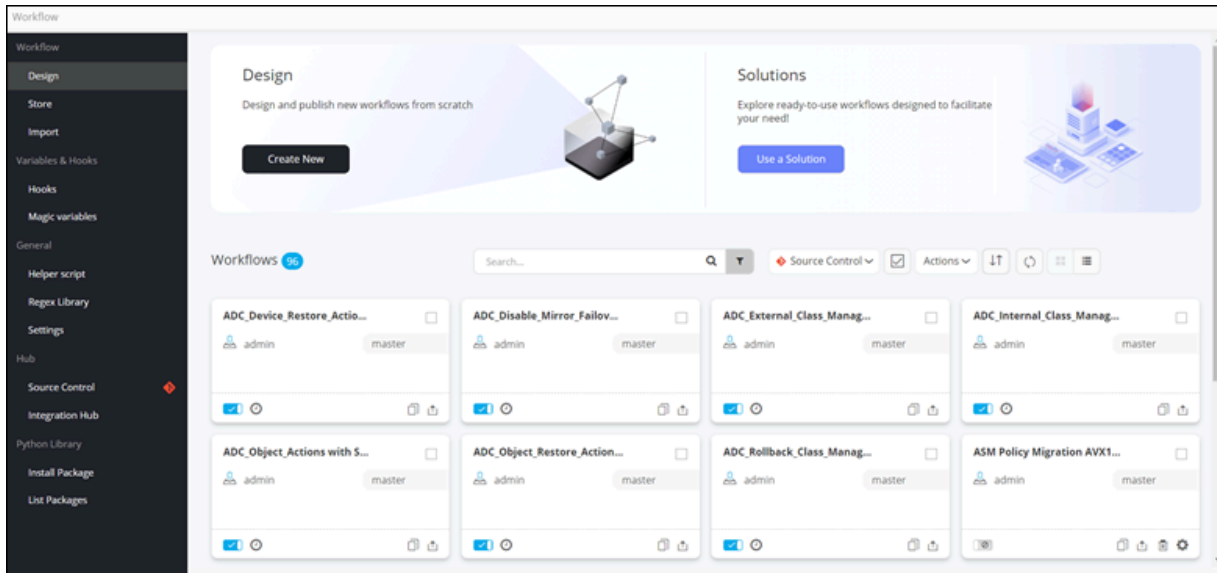
1. Log into AppViewX with valid credentials.



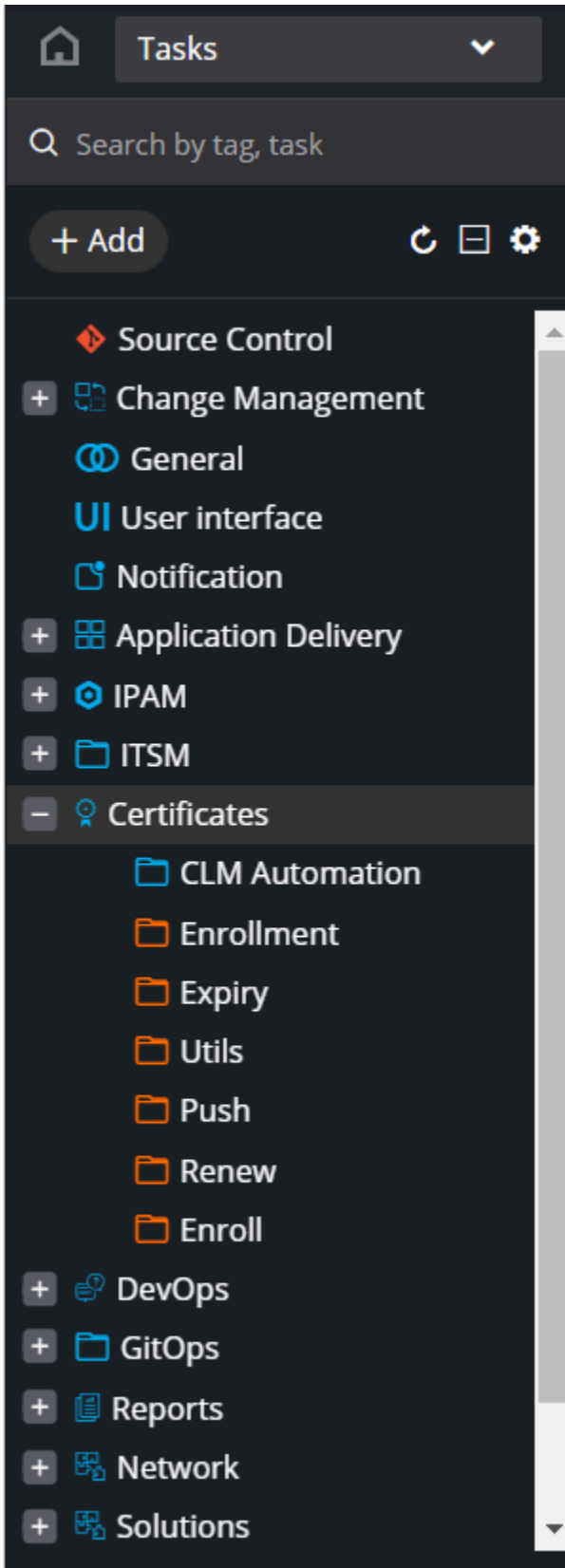
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



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 tasks 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](#)
- [Certificate Expiry Notification based on Certificate Attributes](#)
- [Certificate Expiry Notification - Cert Group Hierarchy](#)
- [Certificate Expiry Notification - Days](#)
- [Certificate Expiry Notification - Devices | Servers](#)
- [Certificate Expiry Notification](#)
- [Update Certificate Attributes](#)
- [Certificate Expiry Notification with JIRA](#)
- [Certificate Expiry Notification with ServiceNow](#)
- [Orphan Certificates Report](#)

Overview

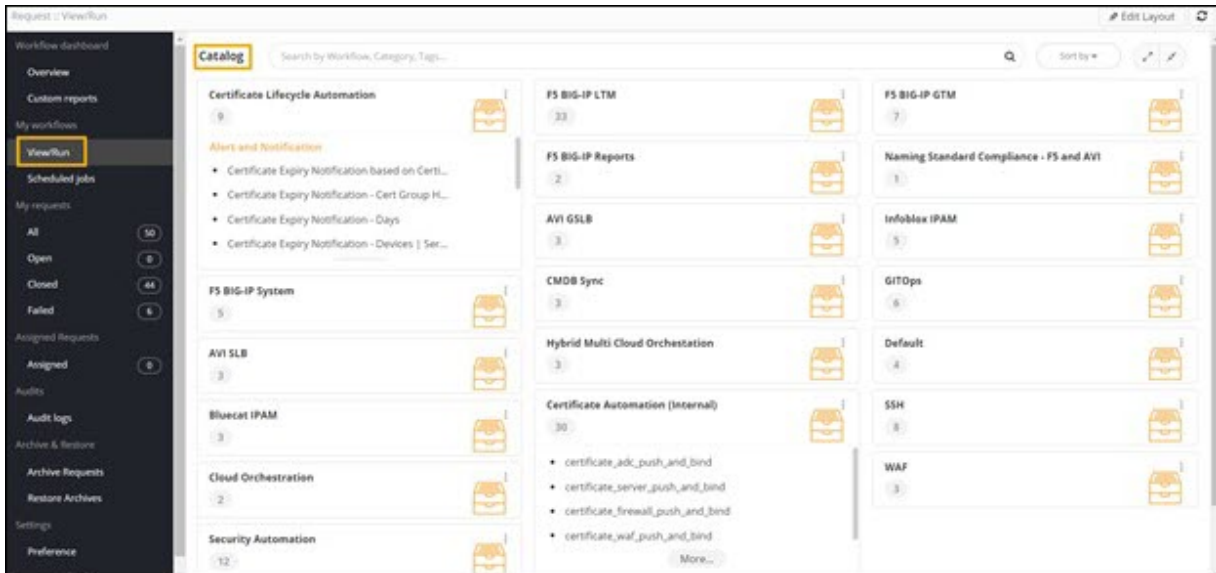
This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. It also enables you to create tickets for expiring certificates on Jira/ServiceNow.



Certificate Expiry Notification based on Certificate Attributes

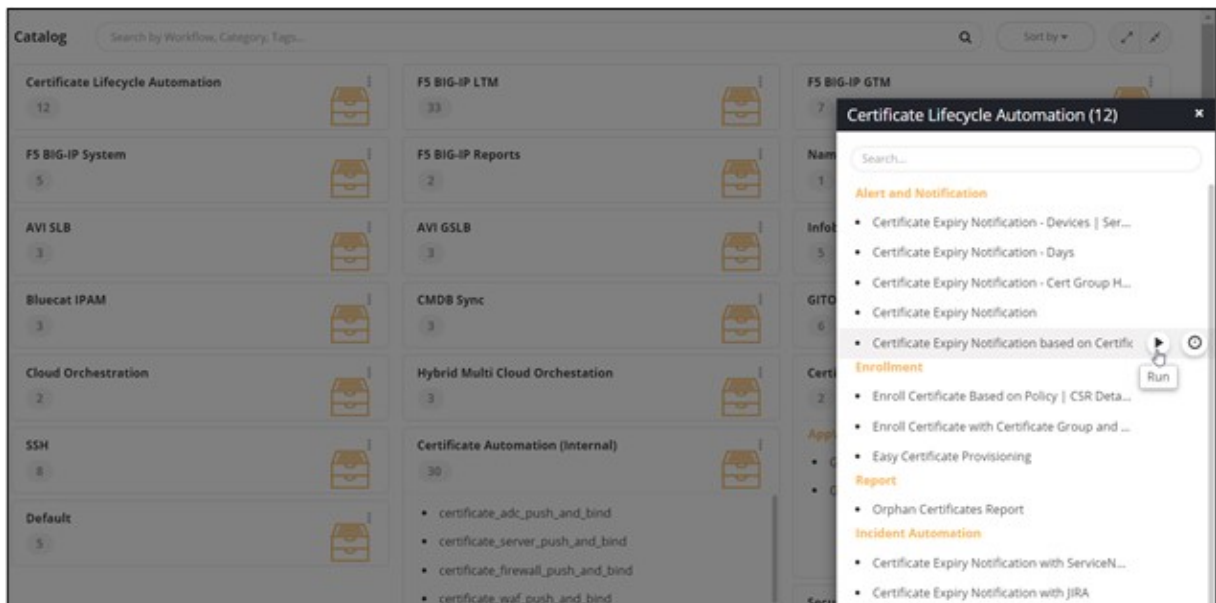
This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.


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	<p>Enter the time frame type from the available options:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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.


^ Notifications

* Email Recipient

* Report Format Email Content CSV Attachment

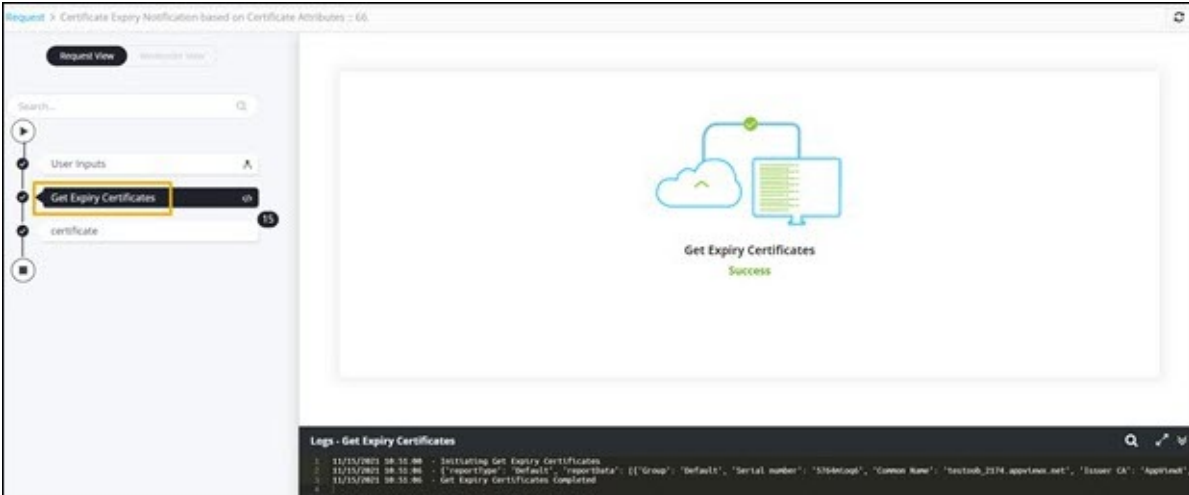
The following table describes the fields under the **Notifications** section:

Field	Description
*Email Recipient	Select the email recipient from the dropdown list.
*Report Format	<p>Select the required checkbox to send the report as:</p> <ul style="list-style-type: none"> • Email content - The report will be sent as Email content. <p>or</p>

Field	Description
	<ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format. <div data-bbox="548 380 1419 468" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: Email Content is the default selection. </div>
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

- **Get Expiry Certificates** task completed.



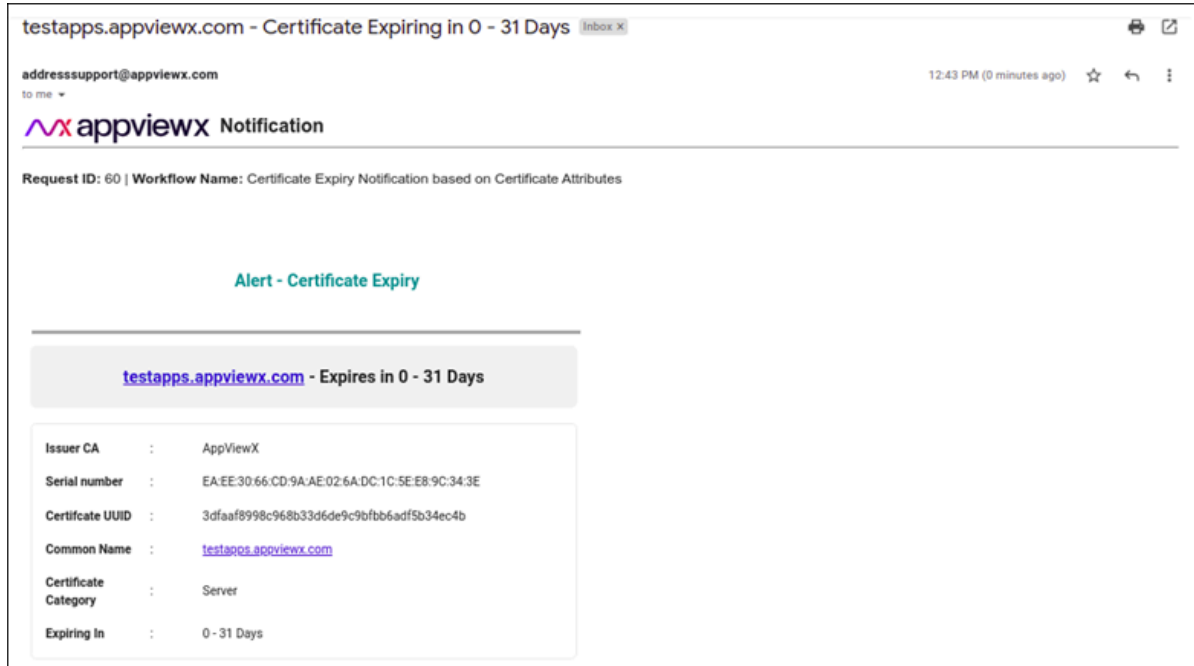
The screenshot displays the 'Request View' of a workflow titled 'Certificate Expiry Notification based on Certificate Attributes - 66'. The workflow diagram on the left shows a sequence of steps: 'User Inputs', 'Get Expiry Certificates' (highlighted with a yellow box and a '13' badge), and 'certificate'. The main workspace shows a 'Success' message for the 'Get Expiry Certificates' task, accompanied by a cloud and server icon. A log window at the bottom provides the following details:

```

Logs - Get Expiry Certificates
1 11/25/2023 08:35:00 - Initiating Get Expiry Certificates
2 11/25/2023 08:35:00 - [Event Type: 'Default', 'EventData': [{"Group": "Default", "Serial number": "5164ncup", "Common Name": "hextab_2174_appview.net", "Issuer CA": "AppView"}]]
3 11/25/2023 08:35:00 - Get Expiry Certificates Completed

```

- Email notification received individually for expiring certificates.

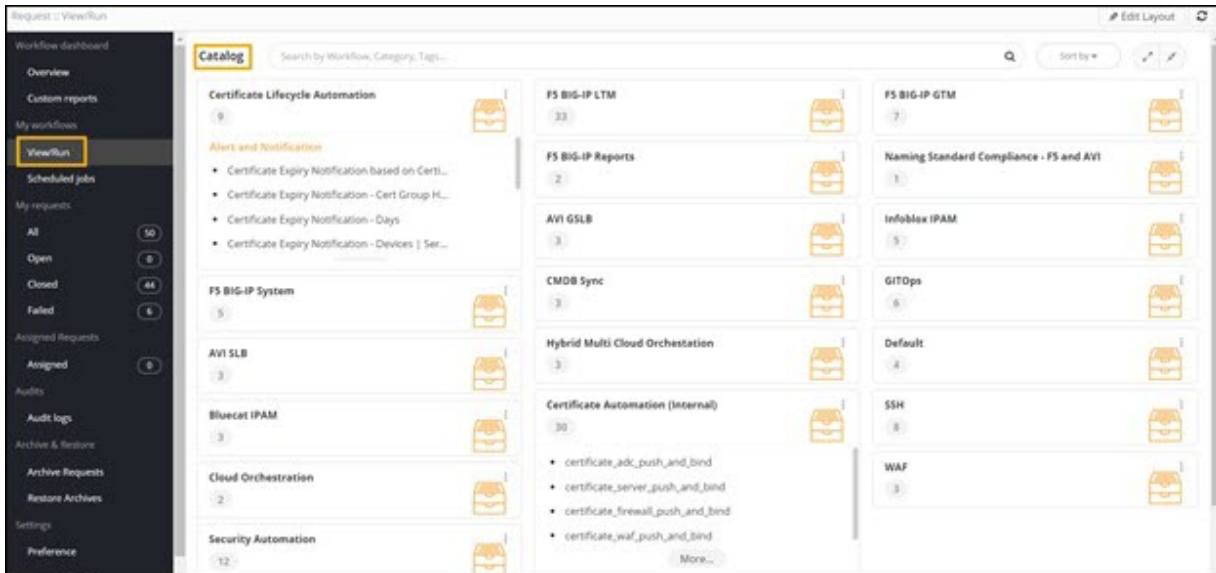




Certificate Expiry Notification - Cert Group Hierarchy

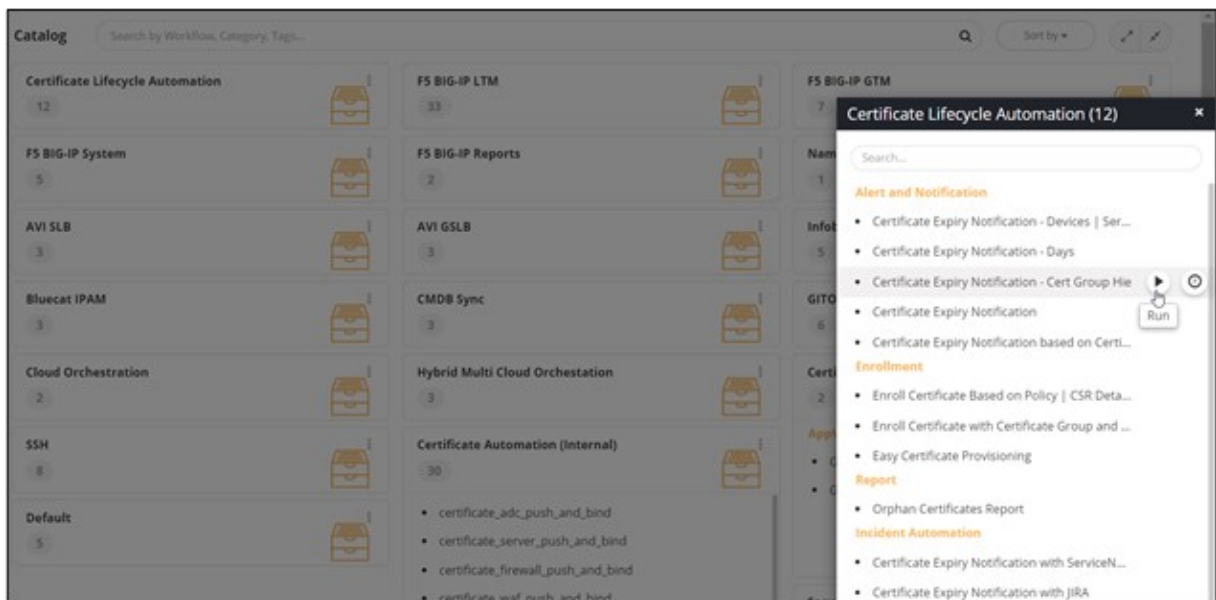
This workflow allows you to send a certificate expiry report notification to the certificate group and its associated hierarchical groups.


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.

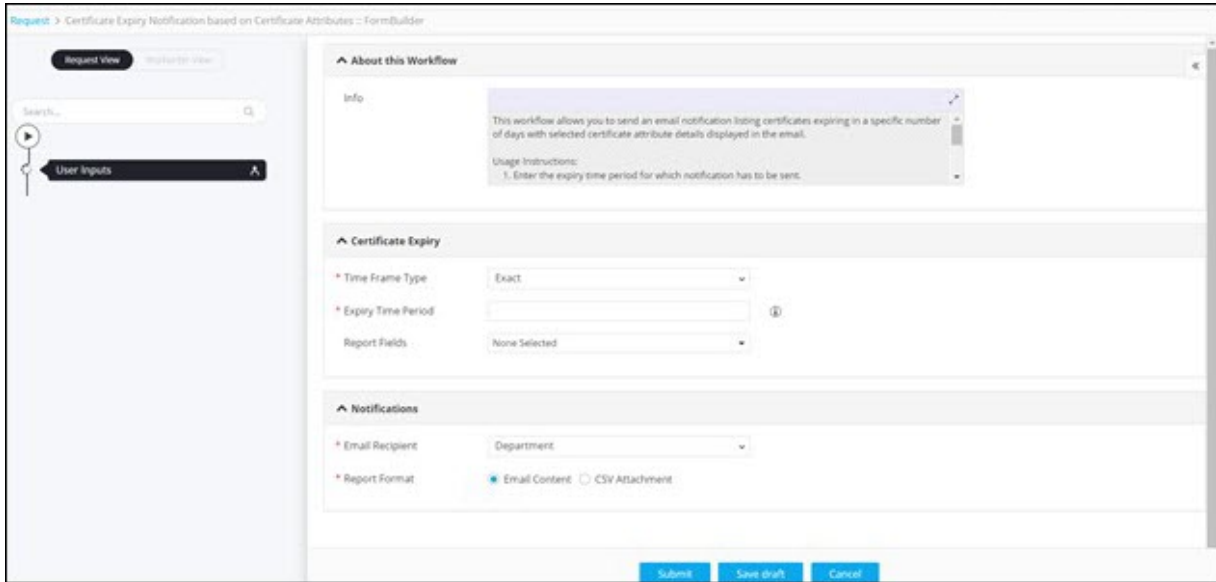


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

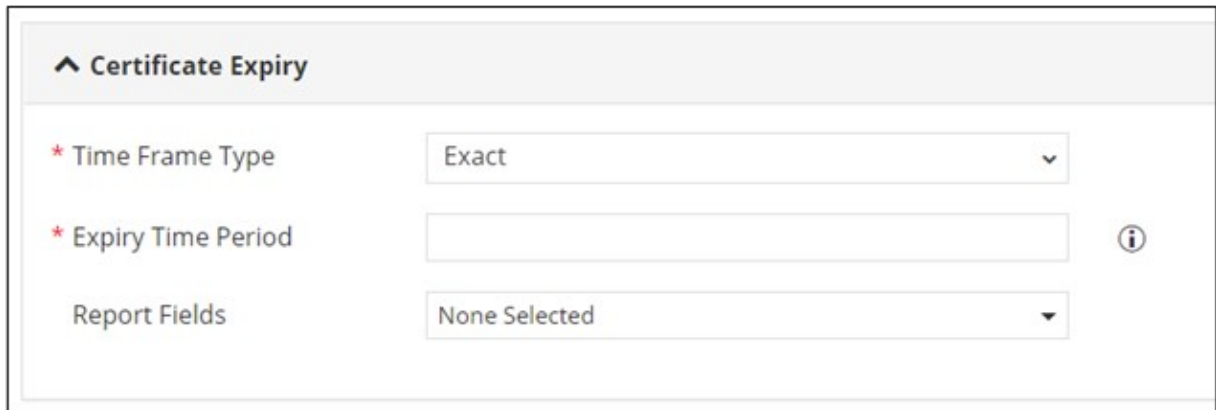


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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	<p>Enter the time frame type from the available options:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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.



^ Notifications

* Notify Parent Group On Off

* Report Format Email Content CSV Attachment

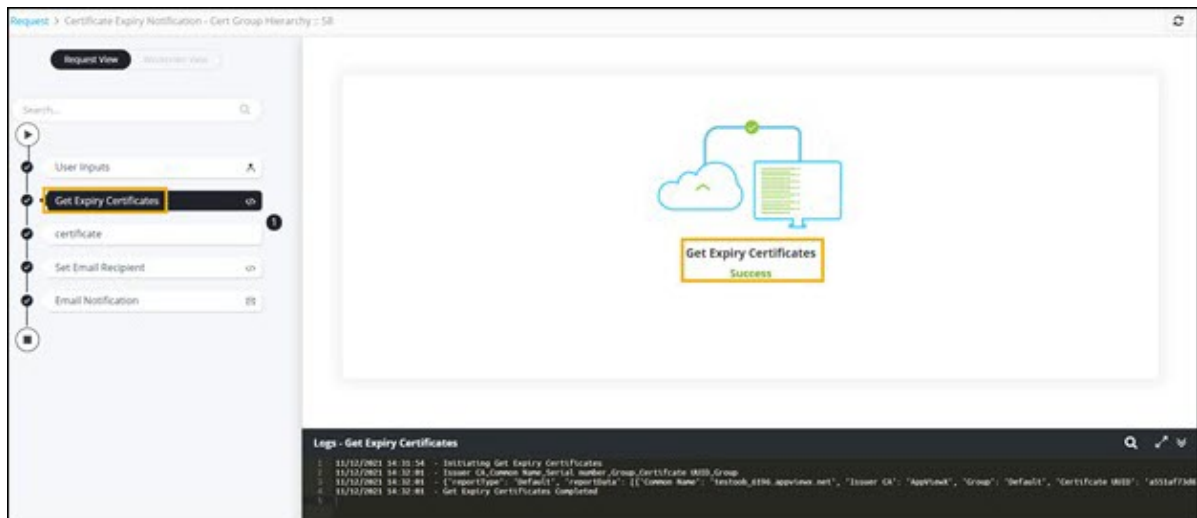
The following table describes the fields under the **Notifications** section:

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

Field	Description
	 Note: On is the default selection.
*Report Format	Select the required checkbox to send the report as: <ul style="list-style-type: none"> • Email content - The report will be sent as Email content. or <ul style="list-style-type: none"> • 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.



The screenshot displays the AppViewX workflow interface. On the left, a task list shows 'Get Expiry Certificates' as the current step. The main workspace shows a 'Success' message for the 'Get Expiry Certificates' task, accompanied by a cloud and server icon. Below the workspace, a log window titled 'Logs - Get Expiry Certificates' shows the following entries:

```

1 11/12/2021 14:32:54 - Initializing Get Expiry Certificates
2 11/12/2021 14:32:54 - Issuer CA, Common Name, Serial Number, Group, Certificate Web, Group
3 11/12/2021 14:32:54 - ("reportType": "Default", "reportData": [{"Common Name": "testlab_@appview.net", "Issuer CA": "AppView", "Group": "Default", "Certificate Web": "d551af72d8"}])
4 11/12/2021 14:32:54 - Get Expiry Certificates Completed
  
```

- Email notification received.

Certificate Expiring in 0 - 60 Days Inbox x

addresssupport@appviewx.com
to me ▾

11:50 AM (0 minutes ago) ☆ ↶ ⋮

appviewx Notification

Request ID: | Workflow Name: Certificate Expiry Notification - Cert Group Hierarchy

Certificate Expiry Notification - Report

Certificate Category	Serial number	Common Name	Group	Issuer CA	Certificate UUID	Expiring In
Server	C5:B1:38:C8:9D:D6:1F:F4:DF:A8: 05:EC:EE:EC:FC:5D	AzureProfileLevelPush. appviewx.comN.JQVQ	Default	AppViewX	ef94228ffdd0cd42d32625c0447f2b be18c9eec4	0 - 60 Days
Server	1F:B5:3D:8D:1D:67:76:22:12:22: C4:E1:4B:AD:64:D0	AzureProfileLevelPush. appviewx.comVJPLY	Default	AppViewX	7eeca946ce5d0f2e986a37f9e690ec 33a96d5ece	0 - 60 Days



Certificate Expiry Notification - Days

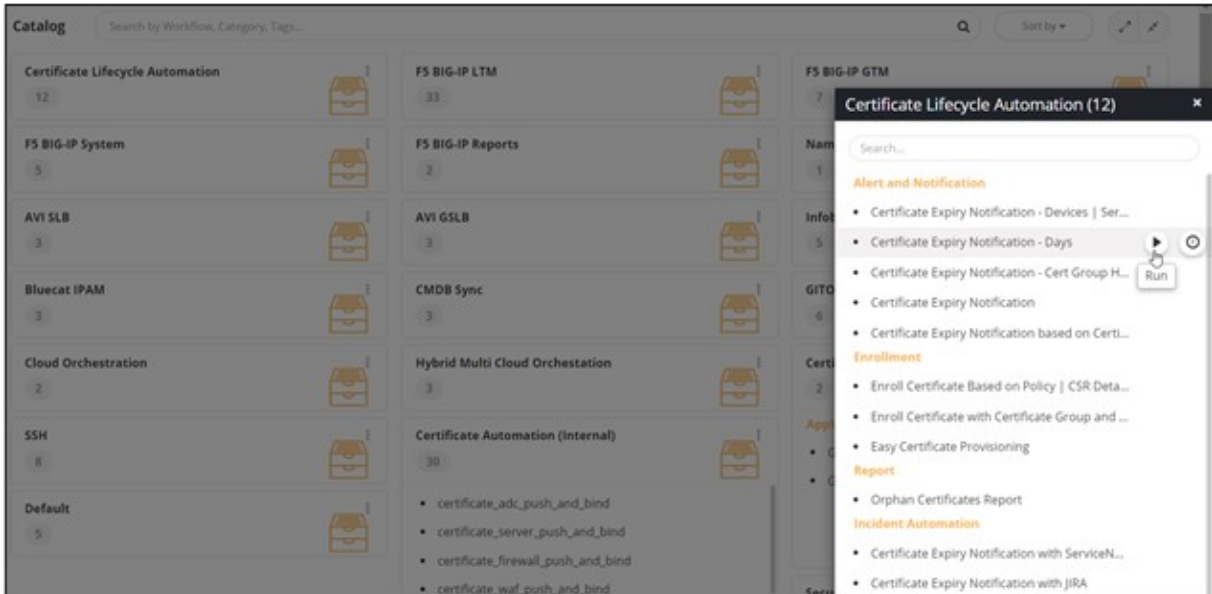
This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.


To trigger this workflow:

1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.

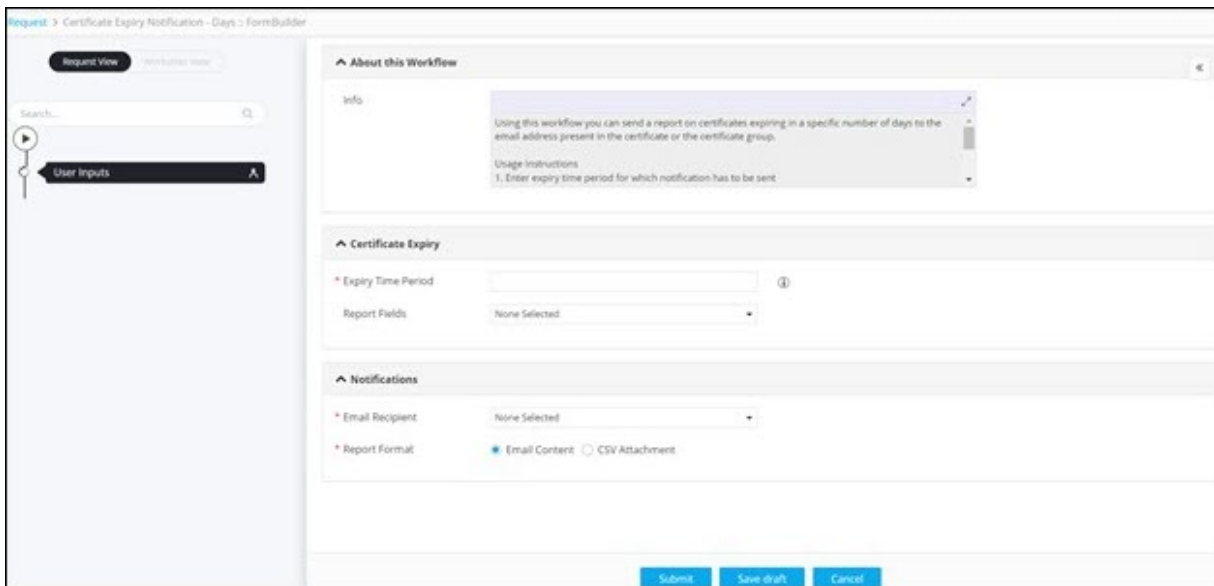
The workflow **Catalog** page is displayed.

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	<p>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.</p> <ul style="list-style-type: none"> • 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.	

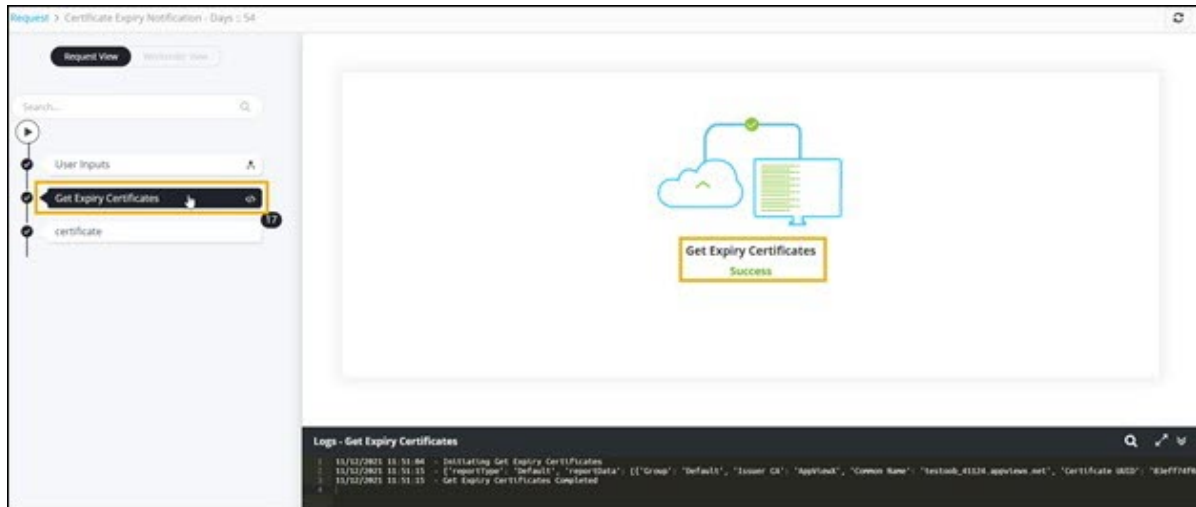
6. Under the **Notifications** section, enter or select the field information as shown.

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

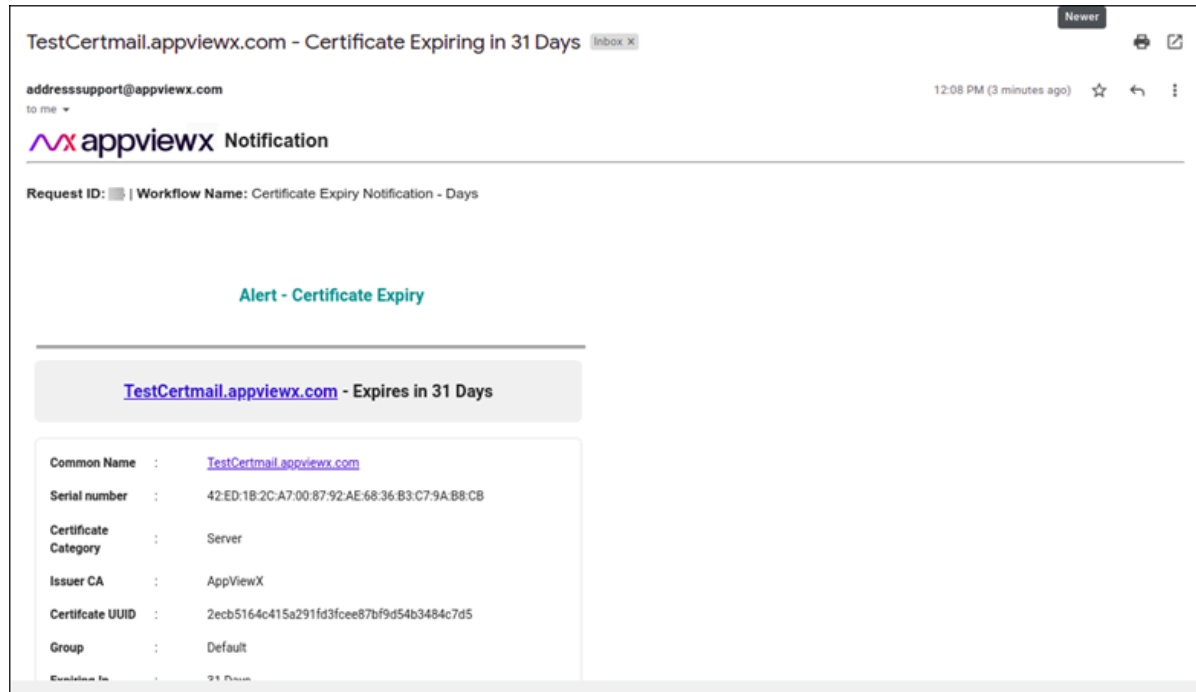
Field	Description
*Email Recipient	<p>Select the required recipient of the notification. You can select:</p> <ul style="list-style-type: none"> • Select all • Certificate Email - The notification will be sent to the email addresses associated with the certificate. • Certificate Group Email - The notification will be sent to the entire certificate group to which the certificate belongs.
*Report Format	<p>Select the required checkbox to send the report as:</p> <ul style="list-style-type: none"> • Email Content - The report will be sent as Email content. <p>or</p> <ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Email Content is the default selection. </div>
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.

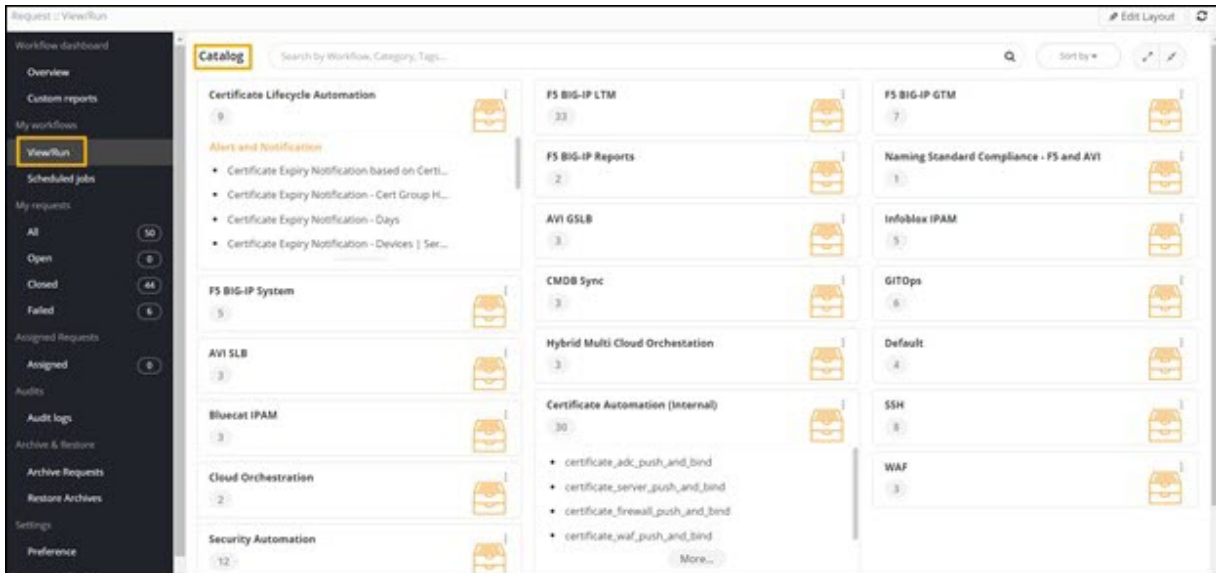




Certificate Expiry Notification - Devices | Servers

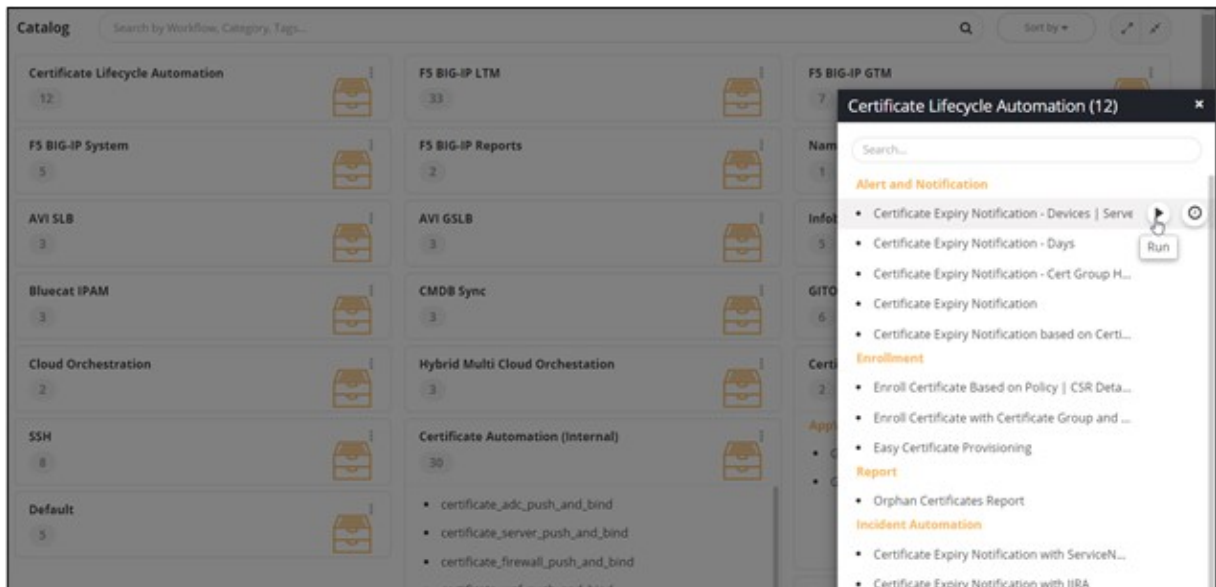
This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

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.

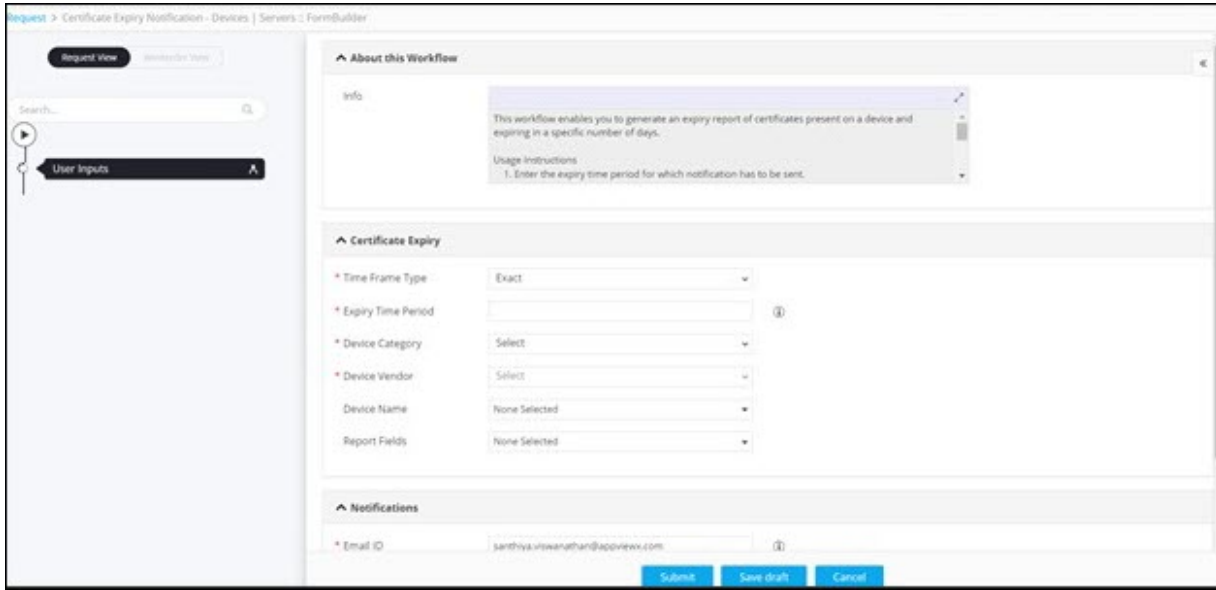


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

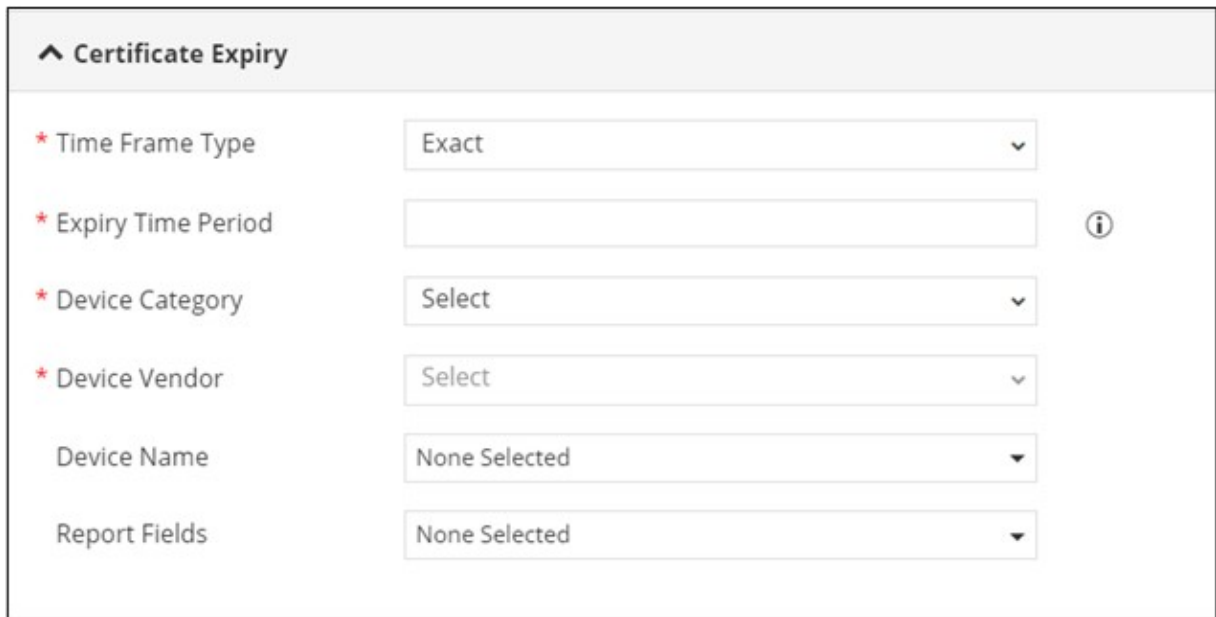


Tip: You can also search for the workflow by typing the workflow name in the search bar.


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	<p>Enter the time frame type from the available options:</p> <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Exact is the default selection. </div>
*Expiry Time Period	<p>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.</p> <ul style="list-style-type: none"> • 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.



^ Notifications

* Email ID ⓘ

CC Email ID ⓘ

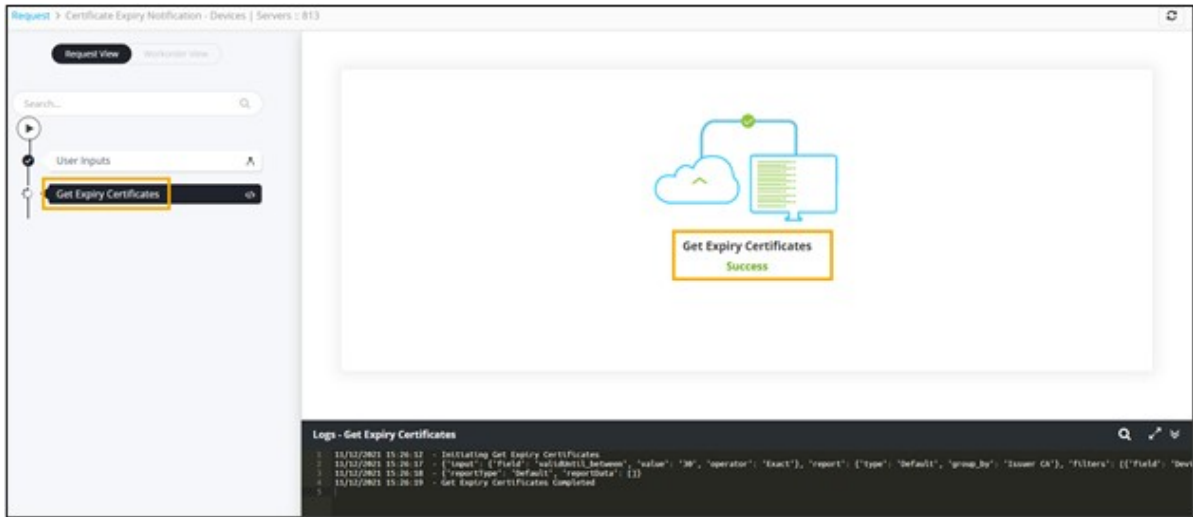
* Report Format Email Content CSV Attachment

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

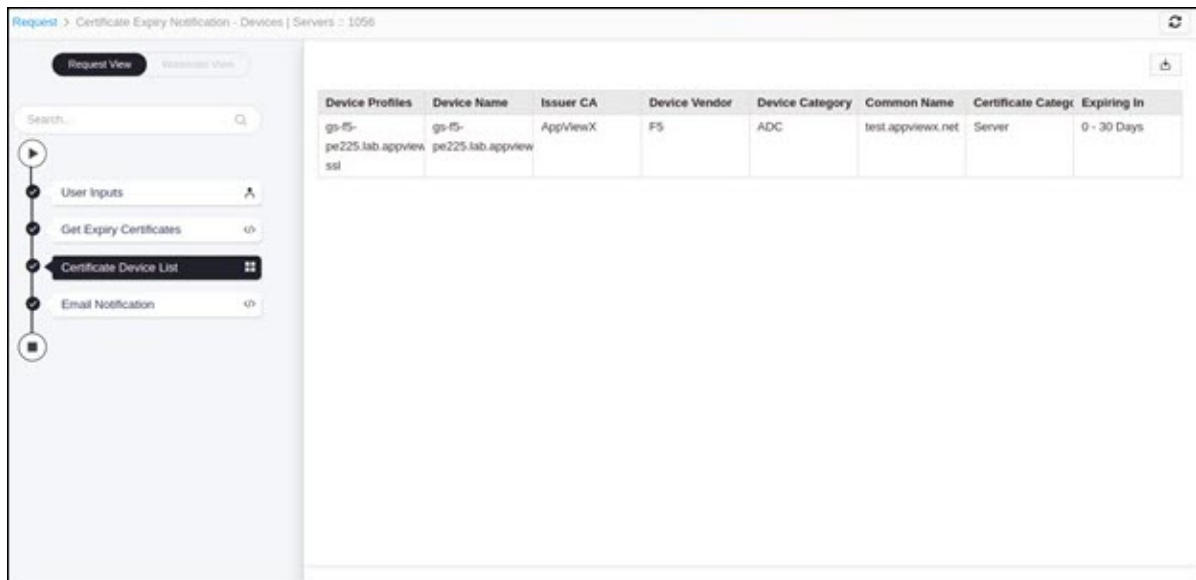
Field	Description
* Email ID	<p>Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: The email id of the logged in user is populated automatically. </div>
CC Email ID	<p>Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.</p>
* Report Format	<p>Select the required checkbox to send the report as:</p> <ul style="list-style-type: none"> • Email Content - The report will be sent as Email content. <p>or</p> <ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Email Content is the default selection. </div>
<p>All Asterisk (*) marked fields are mandatory.</p>	

7. Click **Submit**.

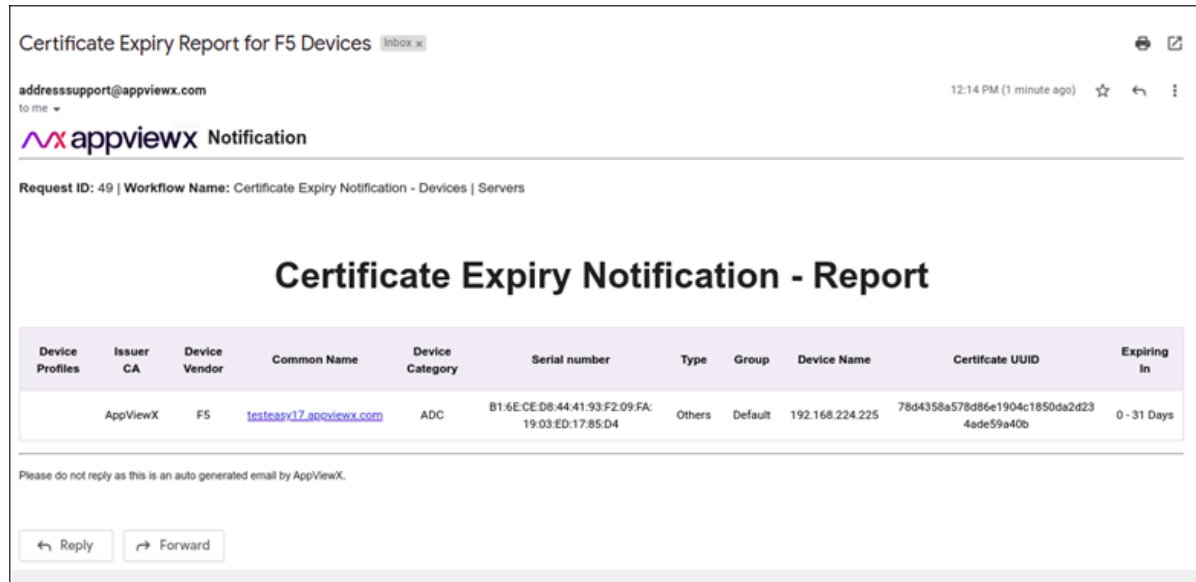
- Get Expiry Certificates task completed.



- Certificate Device list generated.



- Email report received.

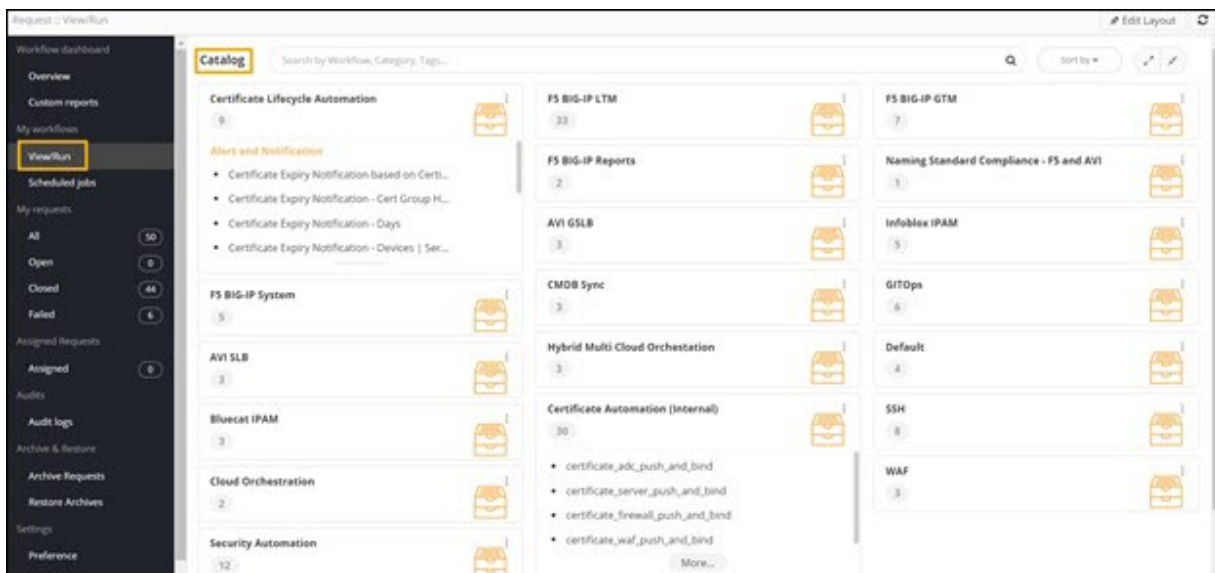




Certificate Expiry Notification

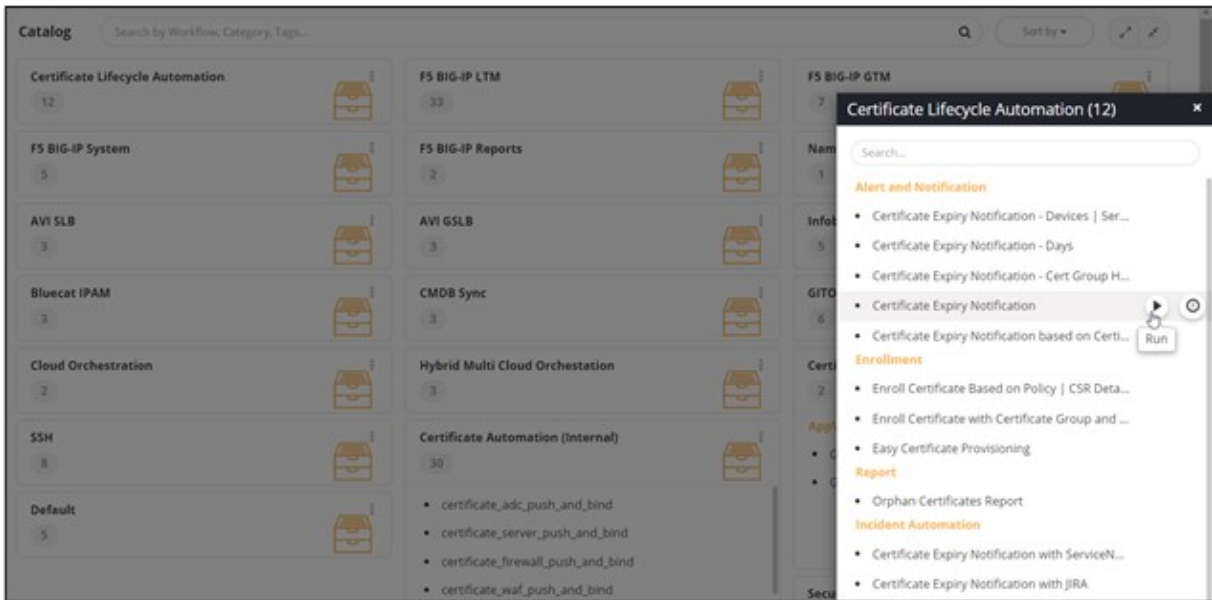
This workflow enables you to generate a report listing certificates expiring in a specific number of days and notify the recipients via email. You can also mention email addresses of the recipients who need to be informed additionally in CC mails.


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.

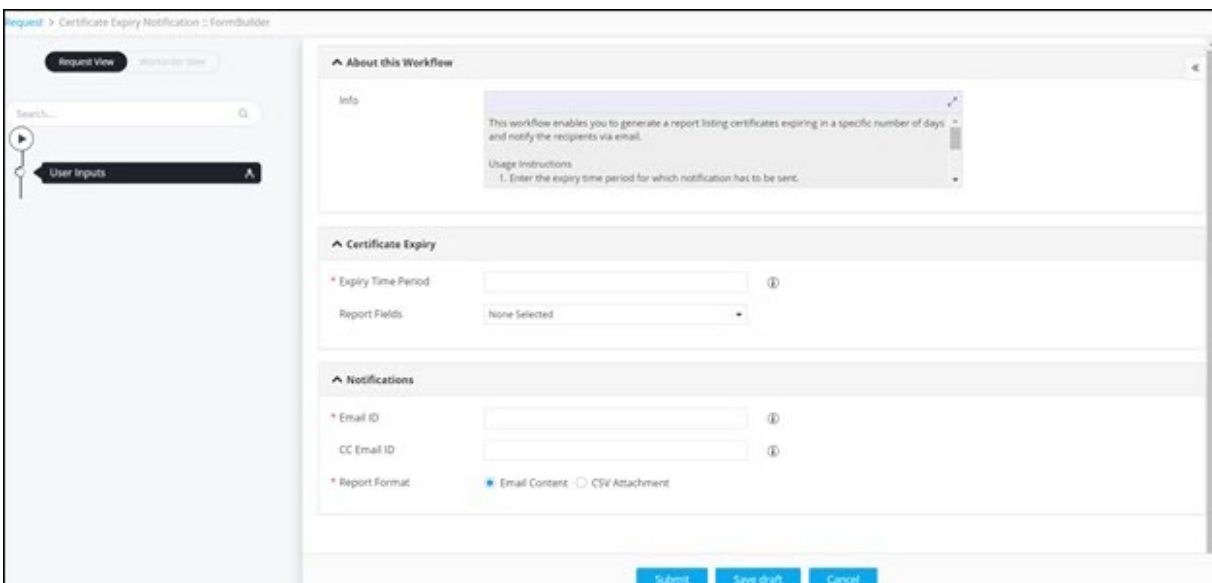


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification** 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	<p>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.</p> <ul style="list-style-type: none"> • 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.	

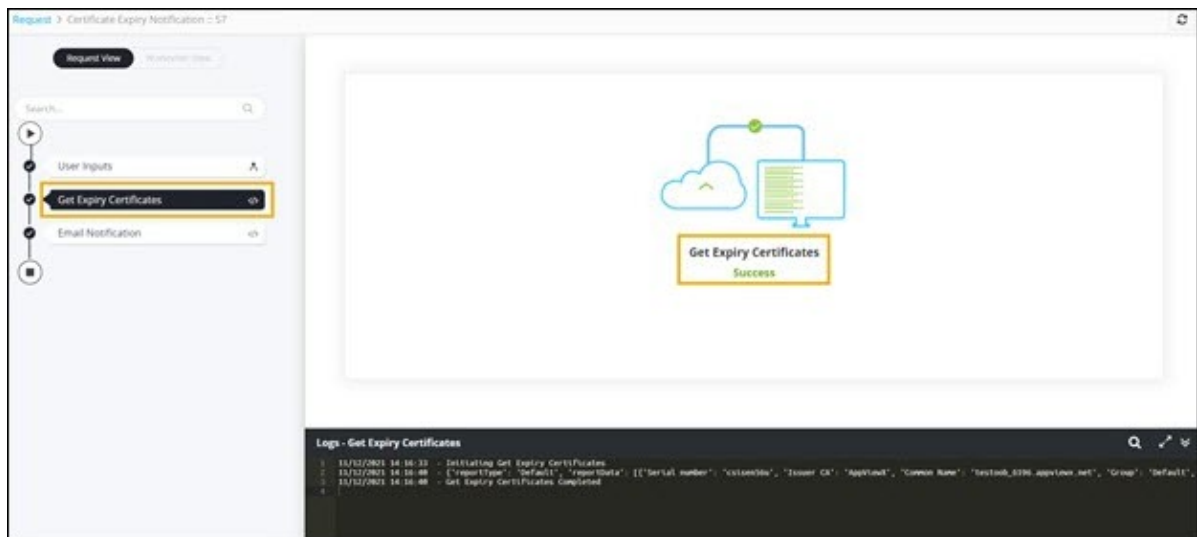
6. Under the **Notifications** section, enter or select the field information as shown.

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

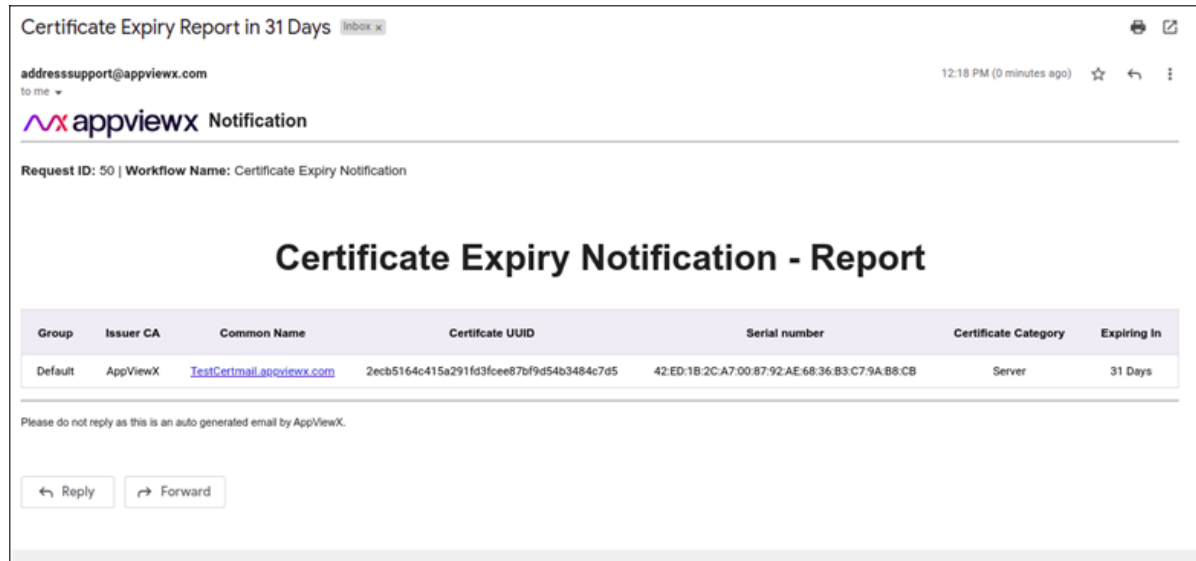
Field	Description
*Email ID	Enter the email address of the recipient in the 'To' field. Comma-separated values can be entered for multiple email addresses.
CC Email ID	Enter the email address of the additional recipients in the 'CC' field. Comma-separated values can be entered for multiple email addresses.
*Report Format	Select the required checkbox to send the report as: <ul style="list-style-type: none"> • Email Content - The report will be sent as Email content. or <ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Email Content is the default selection. </div>
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

- **Get Expiry Certificates** task is executed.



- Email notification received with report as email content.



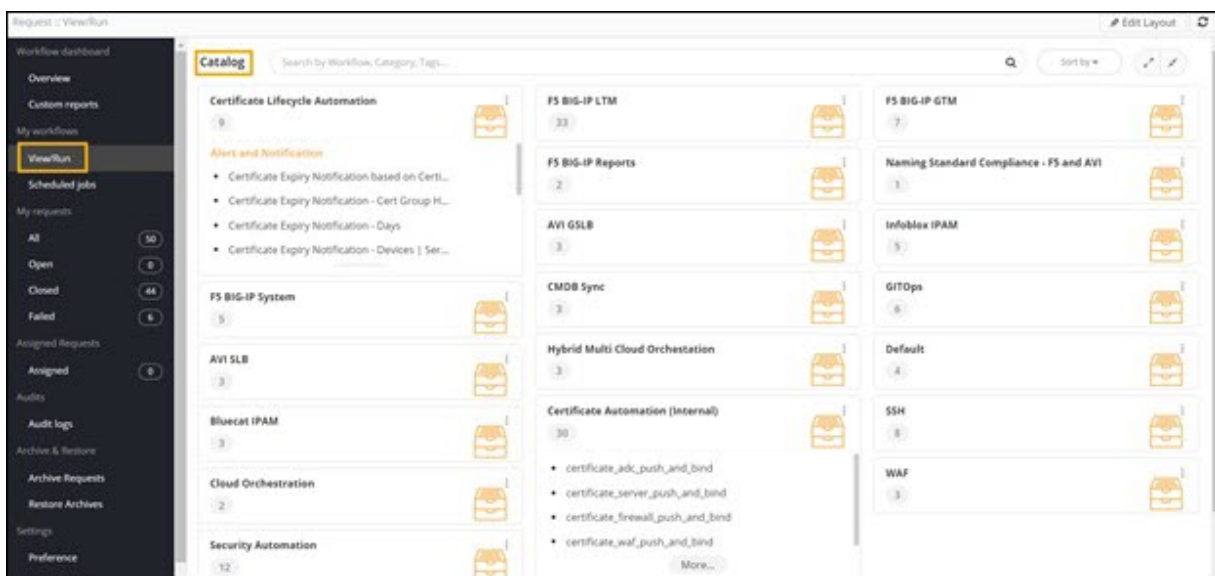
Update Certificate Attributes

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


To trigger this workflow:

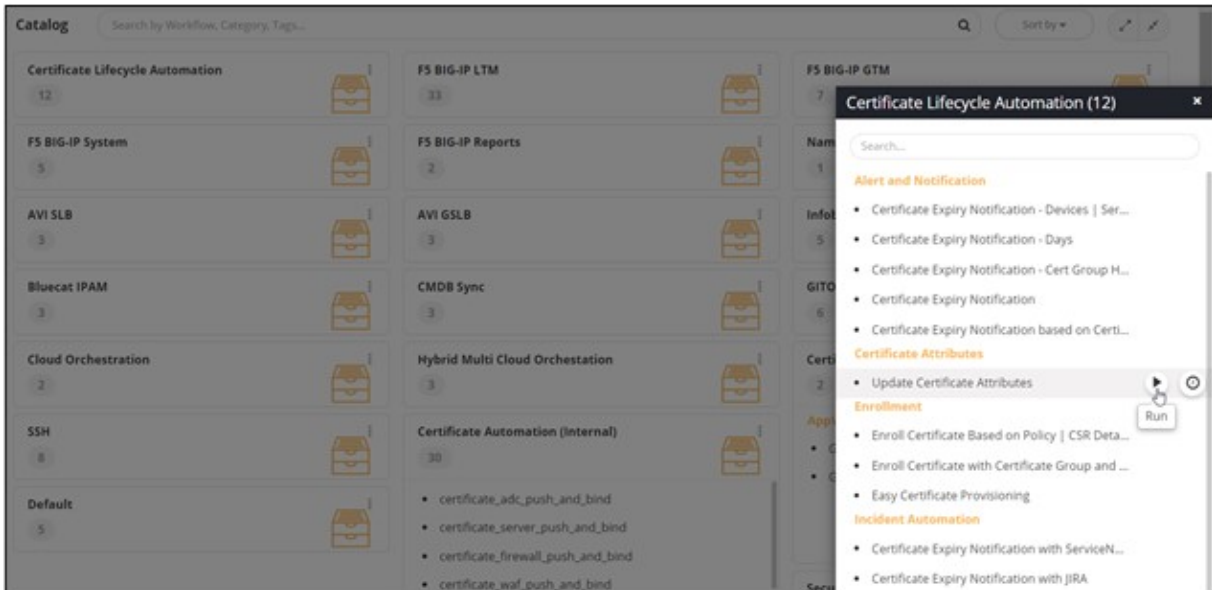
1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.

The workflow **Catalog** page is displayed.



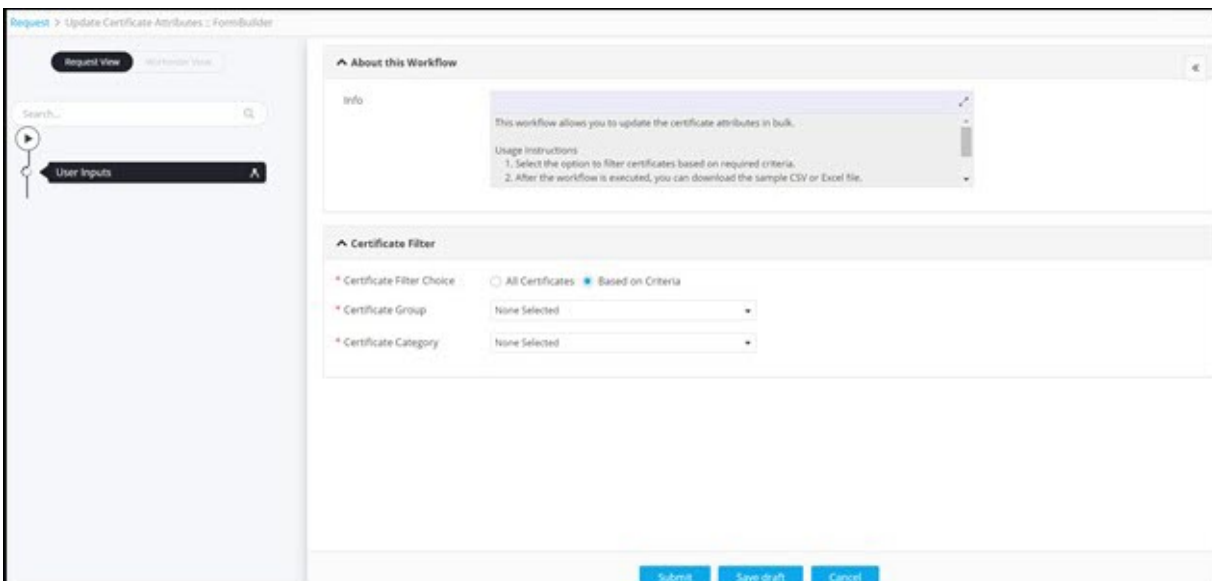
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click  .

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







i **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	<p>Select the required checkbox to fetch</p> <ul style="list-style-type: none"> • All certificates <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin: 5px 0;"> <p> Note: This is the default selection.</p> </div> <ul style="list-style-type: none"> • Based on Criteria <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin: 5px 0;"> <p> Note: Selecting this option will fetch certificates based on criteria such as certificate group and certificate category.</p> </div>
* Certificate Group	<p>Select the appropriate certificate group from the dropdown list.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin: 5px 0;"> <p> Note: This field is displayed only when you select the Based on Criteria option in Certificate Filter Choice.</p> </div>
* Certificate Category	<p>Select the appropriate certificate category from the dropdown list.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin: 5px 0;"> <p> Note: This field is displayed only when you select the Based on Criteria option in Certificate Filter Choice.</p> </div>
All asterisk (*) marked fields are mandatory.	

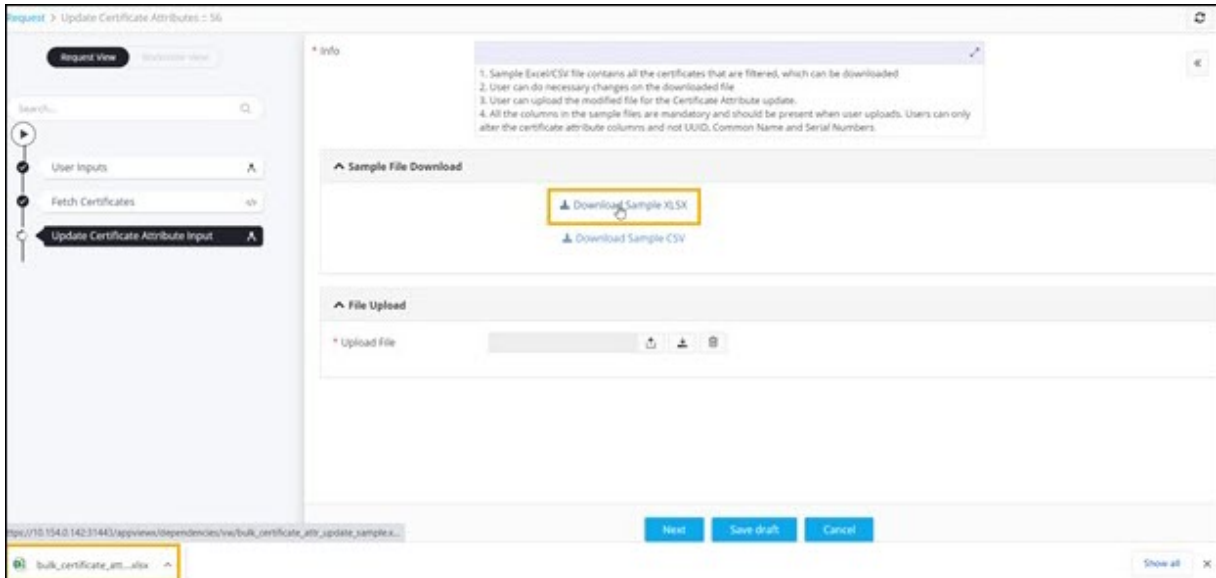
5. Click **Submit**.


Fetch Certificates task is executed.

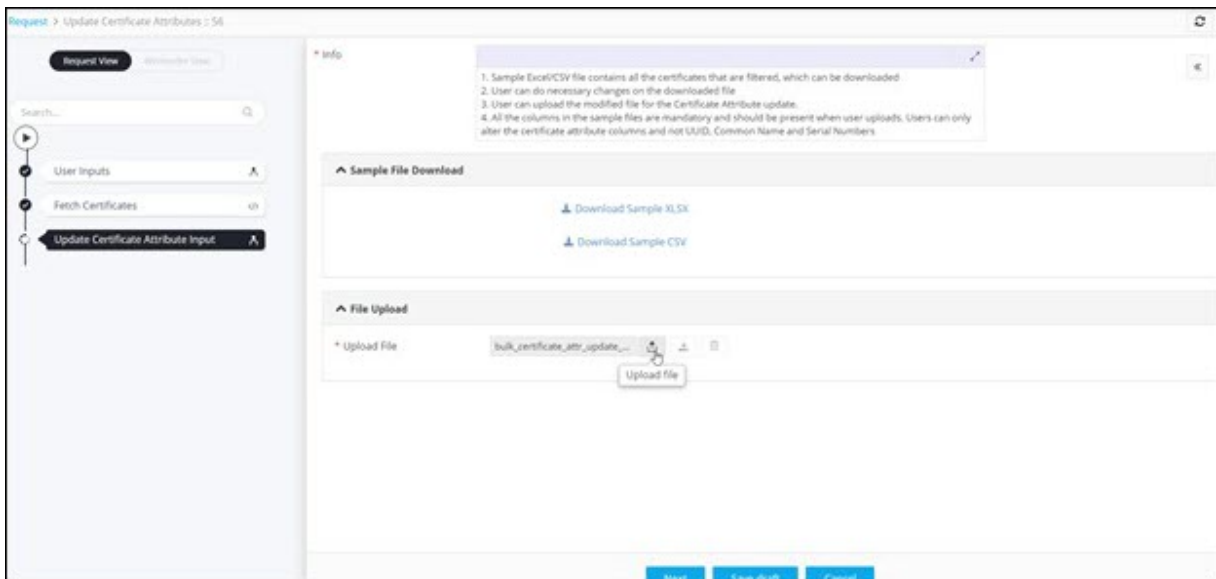


6. Select the appropriate option for downloading the file as a CSV or Excel file.

The file is downloaded to your device.



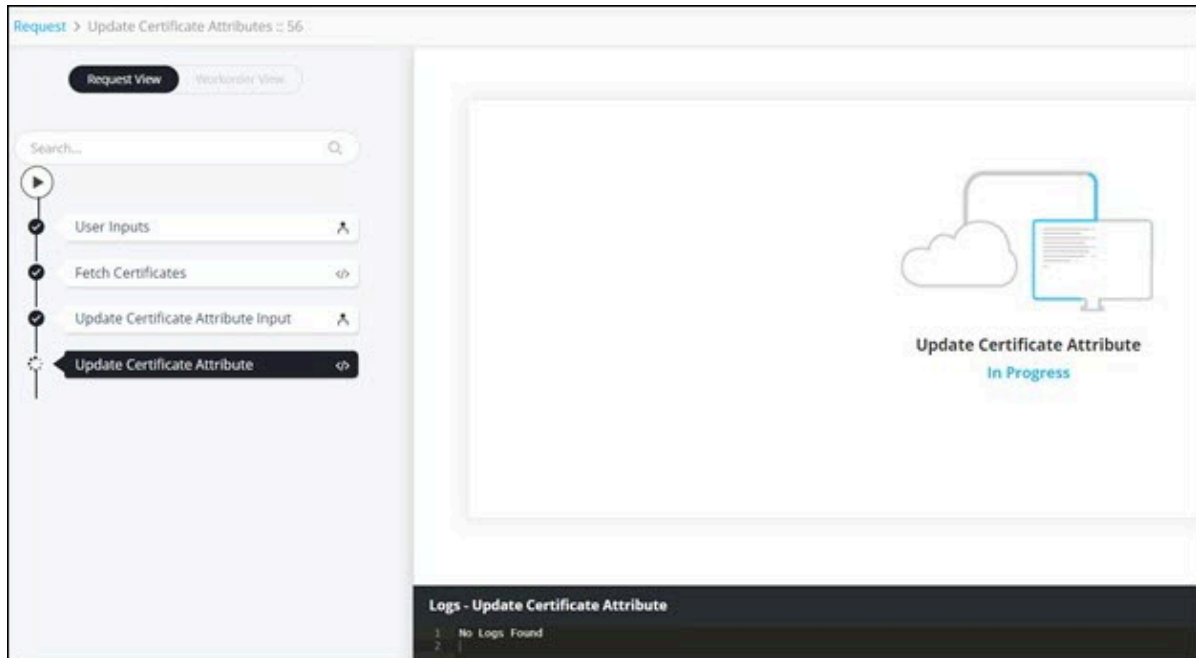
7. Once you have updated the certificate attributes in the downloaded file, under **File Upload**, click  to upload the modified file.



8. Click **Next**

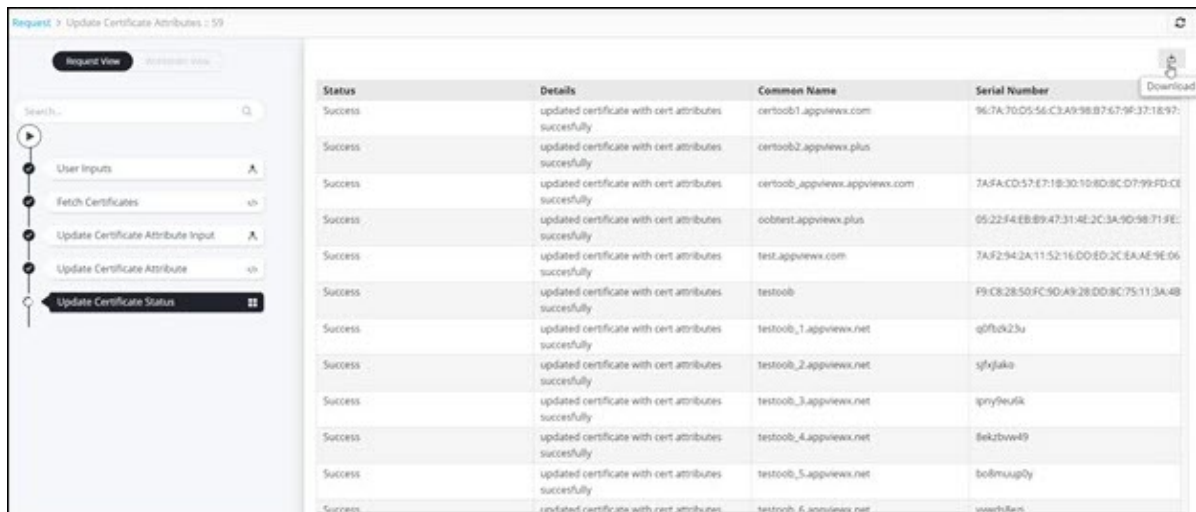
9. In the **Confirmation** pop-up window, click **Ok**.

- Update Certificate Attributes task in progress.



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

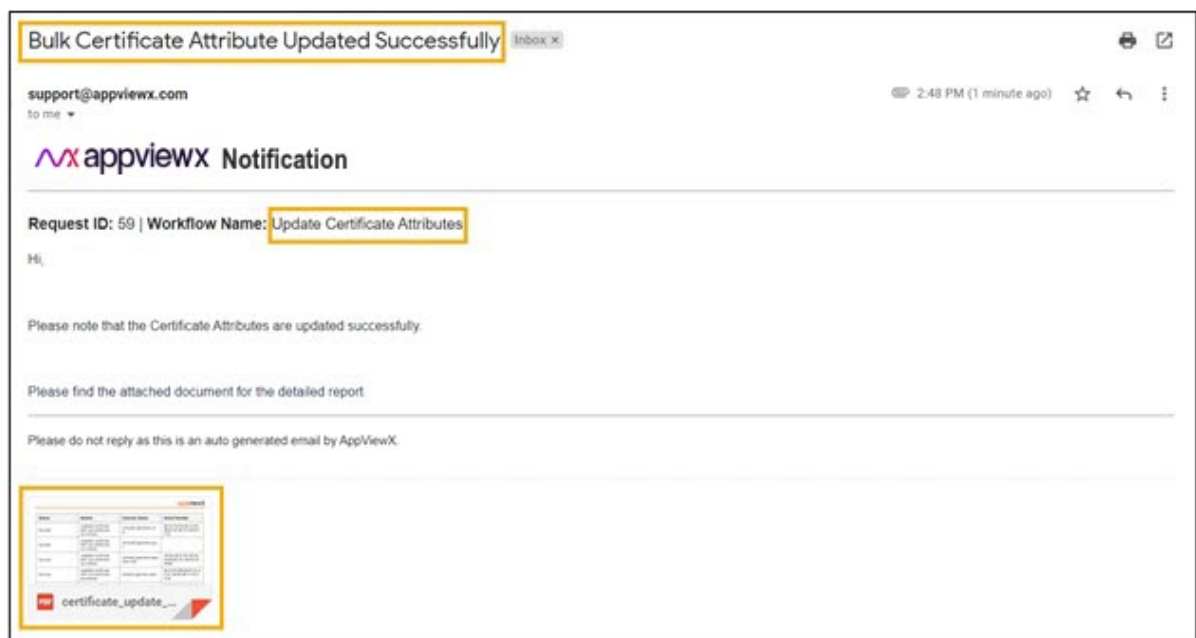
click  .



- Email notification sent successfully.



- Email with report received.

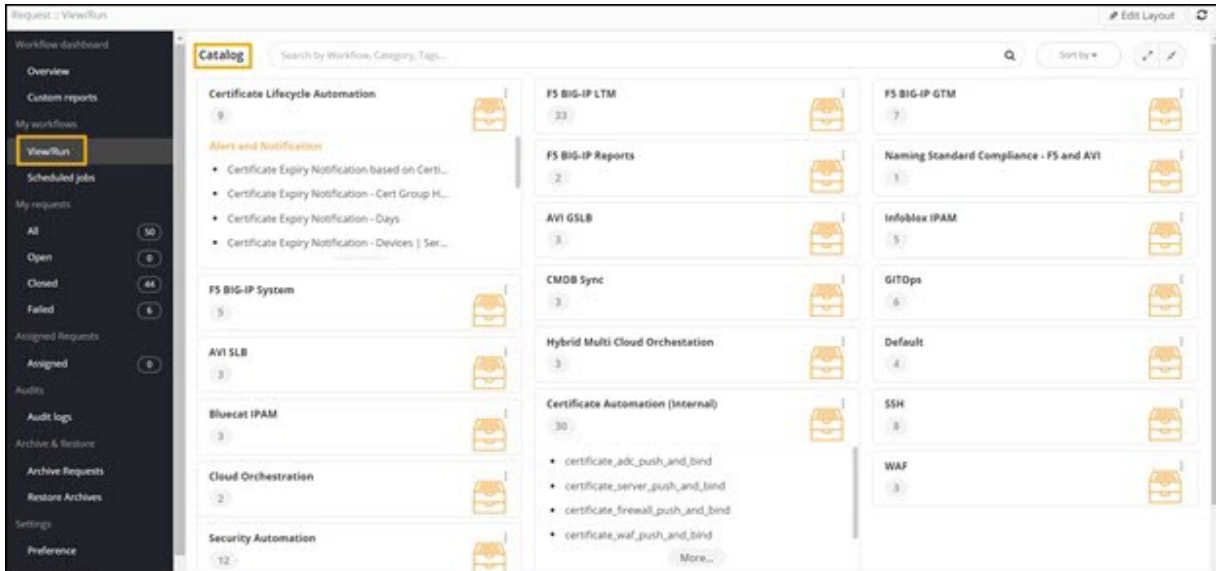




Certificate Expiry Notification with JIRA

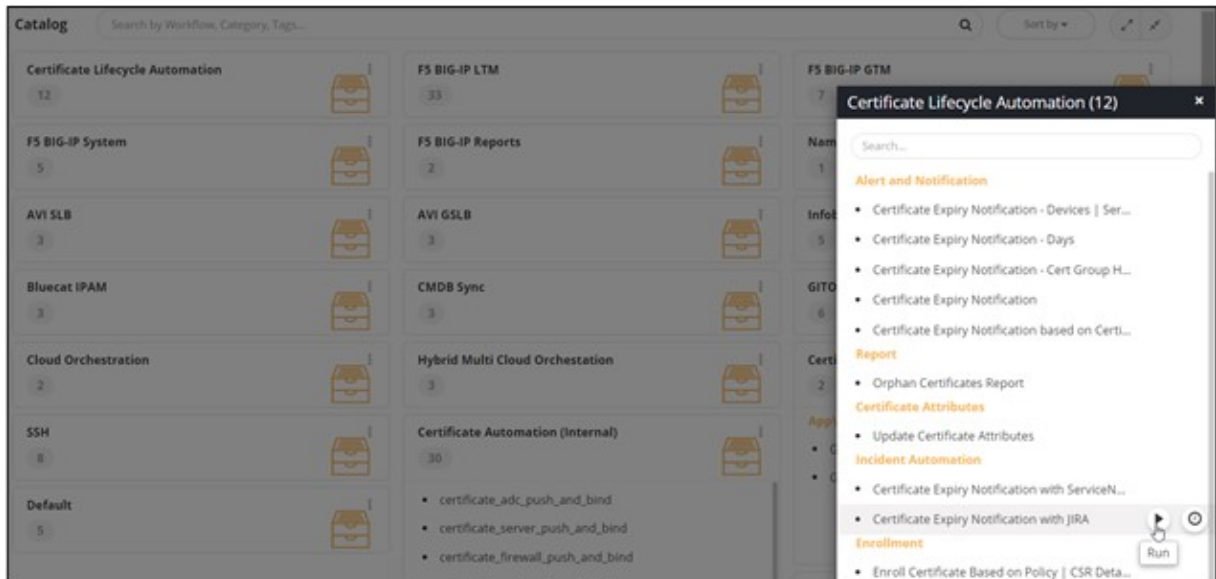
This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.

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.

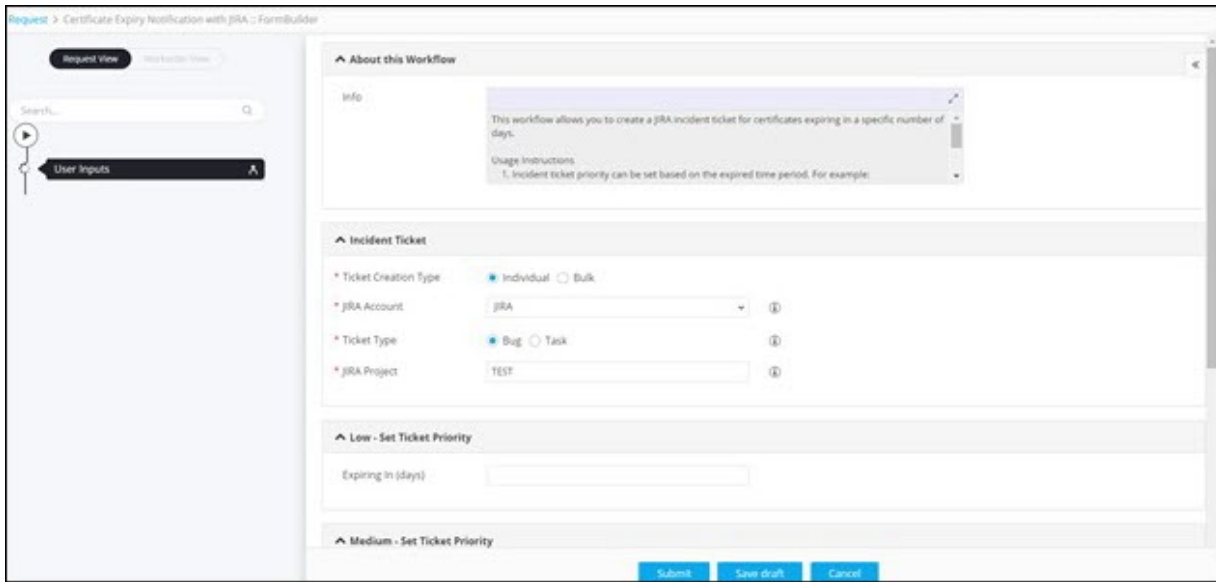


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

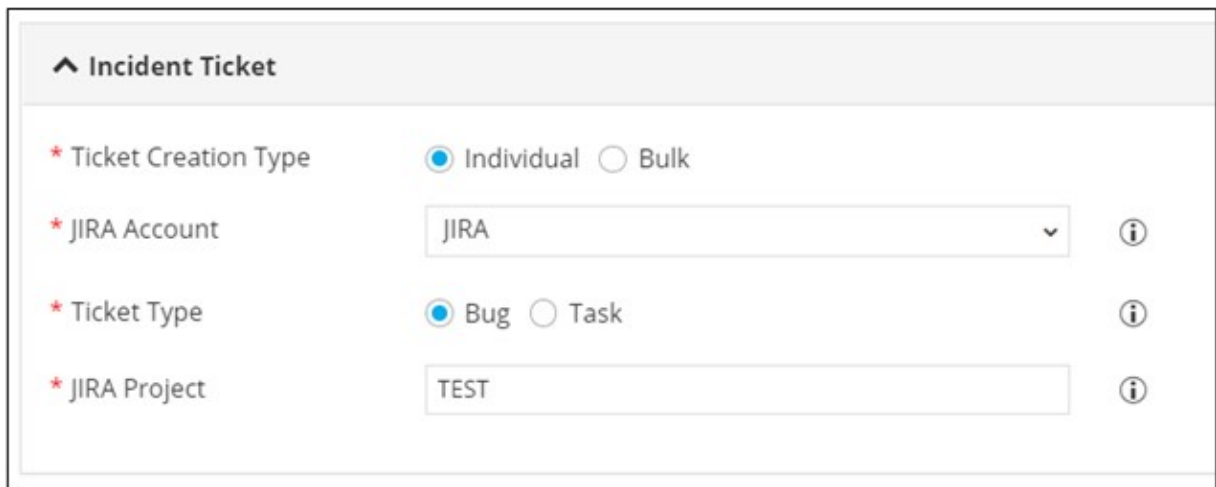


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.	

- 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.
- 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.
- 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.
- Under the **Description Fields** section, select certificate attributes from the dropdown that will be displayed in the JIRA issue description.



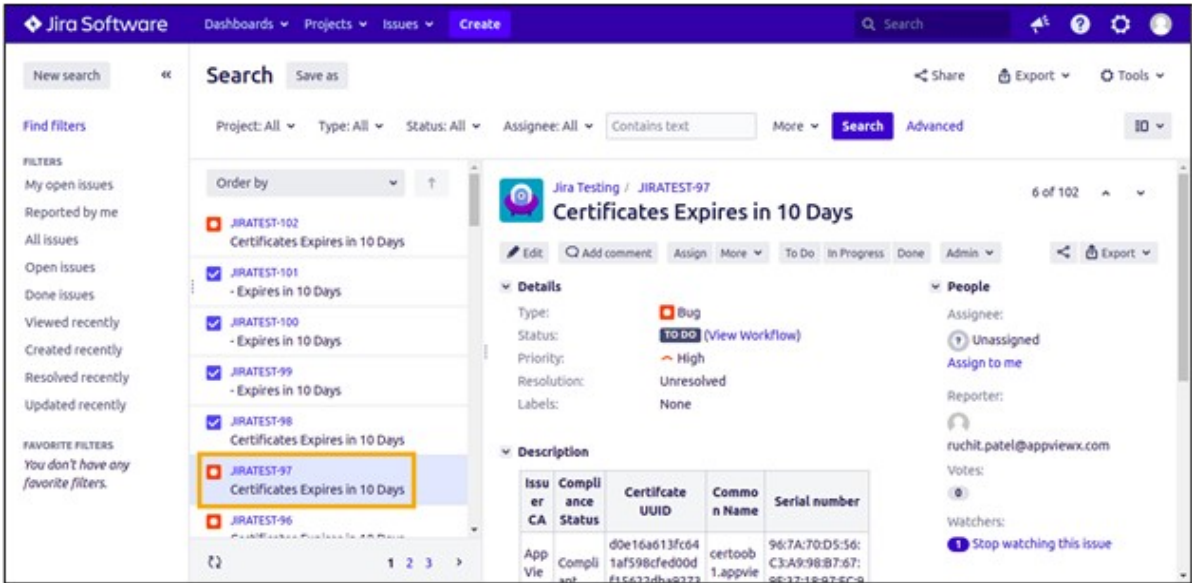
Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

- Click **Submit**.

- JIRA ticket creation Summary.



- Ticket created on Jira.



The screenshot shows a Jira Software issue page for the project 'Jira Testing'. The issue title is 'Certificates Expires in 10 Days' and the issue ID is 'JIRATEST-97'. The issue is a 'Bug' with a 'High' priority and a 'TO DO' status. The resolution is 'Unresolved'. The description section contains a table with the following data:

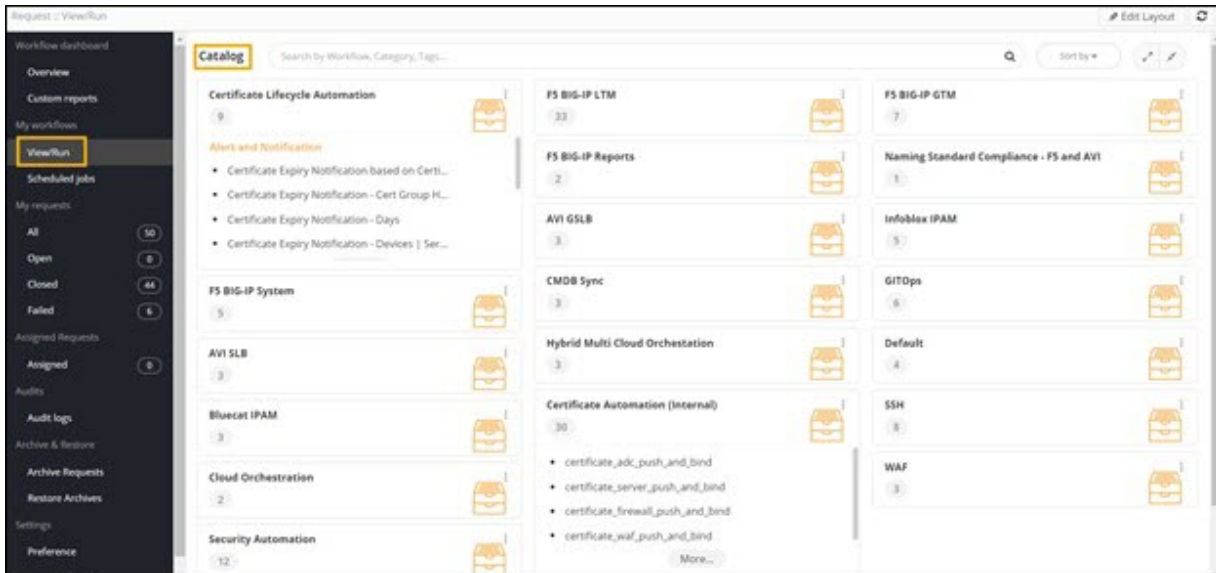
Issue r CA	Compliance Status	Certificate UUID	Common Name	Serial number
AppViewX	Compliant	d0e16a613fc641af598cfed00df15622dba92733	certoob1.ap pviewx.com	96:7A:70:D5:56:C3:A9:98: B7:67:9F:37:18:97:FC:91
AppViewX	Compliant	d0e16a613fc641af598cfed00df15622dba92733	certoob1.ap pviewx.com	96:7A:70:D5:56:C3:A9:98: B7:67:9F:37:18:97:FC:91
AppViewX	Compliant	d0e16a613fc641af598cfed00df15622dba92733	certoob1.ap pviewx.com	96:7A:70:D5:56:C3:A9:98: B7:67:9F:37:18:97:FC:91



Certificate Expiry Notification with ServiceNow

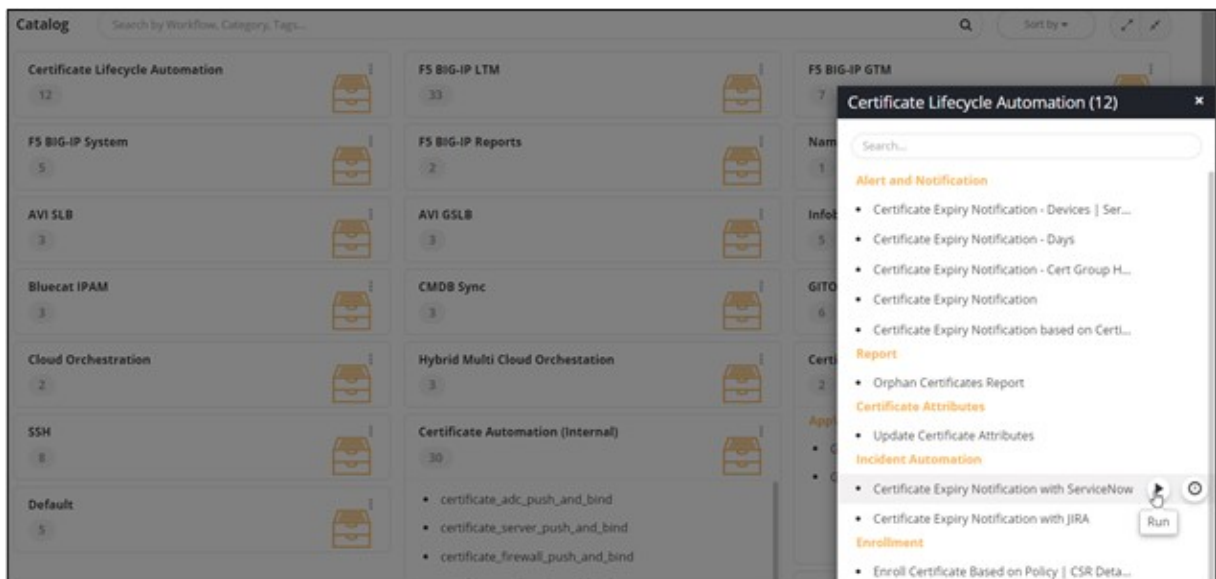
This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.

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.

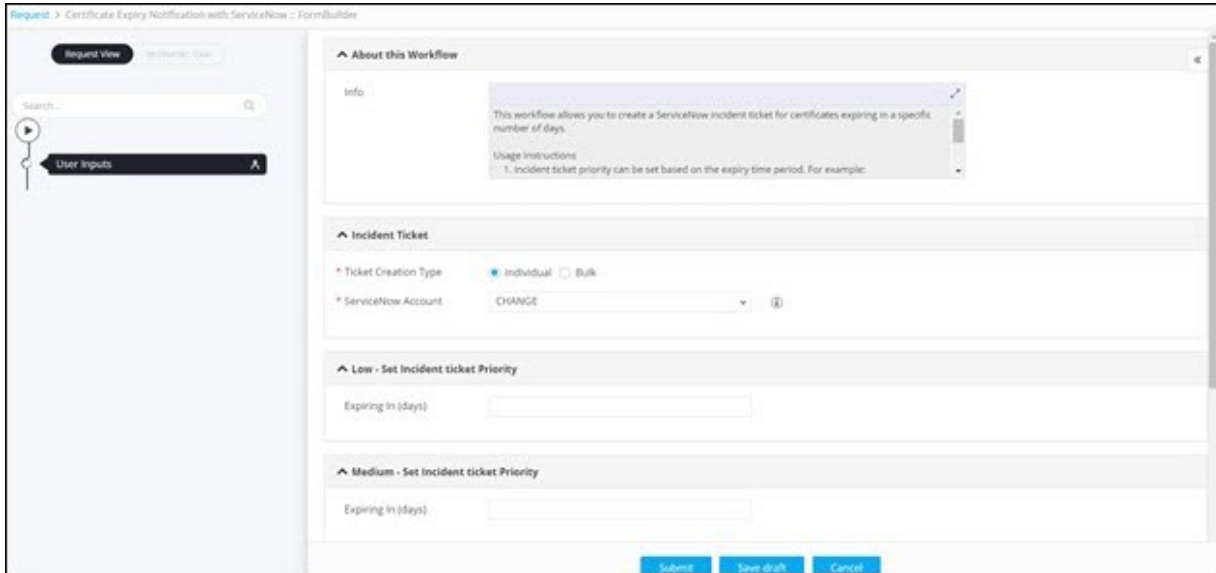


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

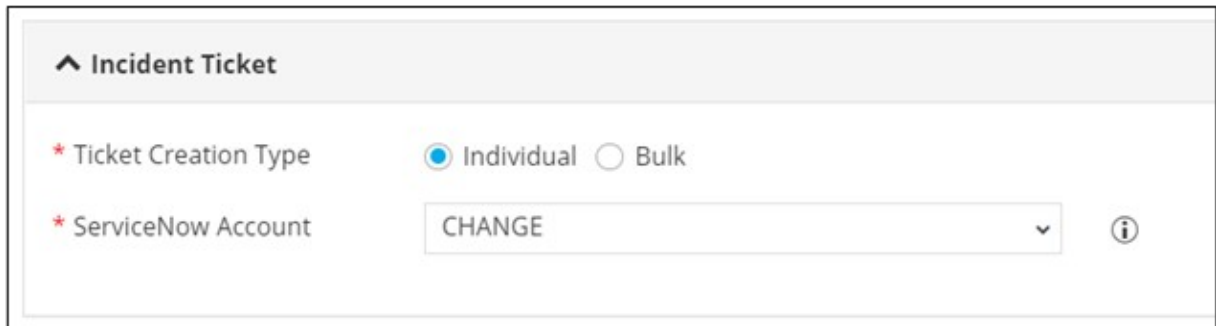


Tip: You can also search for the workflow by typing the workflow name in the search bar.


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	<p>Select Ticket Creation Type as:</p> <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Individual is the default selection. </div>
*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.	

- 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.
- 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.
- 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.
- 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.

servicenow Service Management

Global System Administrator

Incident INC0014750

Number INC0014750

Caller

Category Inquiry / Help

Subcategory --None--

Business service

Service offering

Configuration item

Contact type Phone

State New

Impact 1 - High

Urgency 1 - High

Priority 1 - Critical

Assignment group

Assigned to

Short description Certificates - Expires in 10 Days

Description

Issuer CA: AppViewX
Certificate Category: Server
Common Name: certtoob_78830
Group: Default

Issuer CA: AppViewX
Certificate Category: Server
Common Name: certtoob_10851
Group: Default

Incidents New Search Created Search

All > Active = true

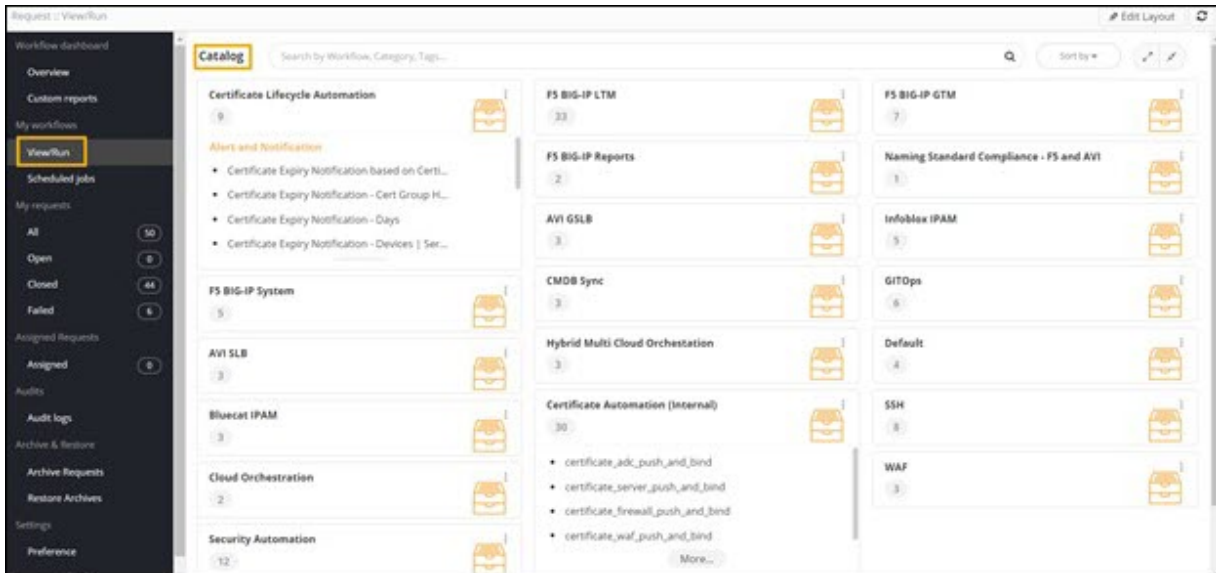
	Number	Caller	Short description	Category	Priority	State	Assignment group	Assigned to	Created
	INC0014751	(empty)	certtoob1.appviewx.com - Expires in 10 Days	Inquiry / Help	1 - Critical	New	(empty)	(empty)	2021 03:51
	INC0014750	(empty)	Certificates - Expires in 10 Days	Inquiry / Help	1 - Critical	New	(empty)	(empty)	2021 04:21



Orphan Certificates Report

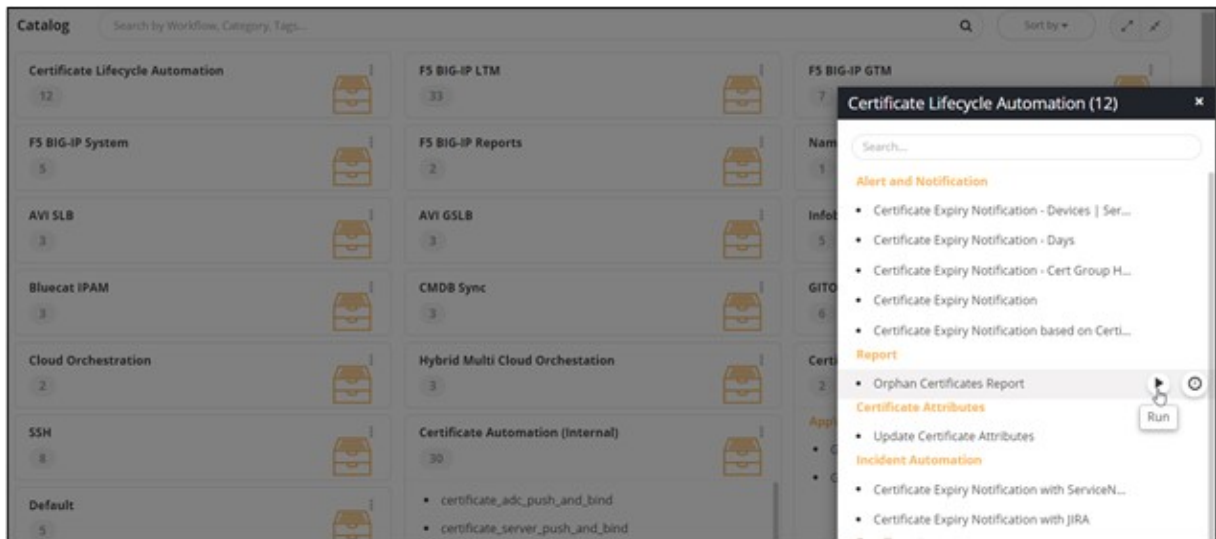
This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.


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 screenshot shows the 'Notifications' section with the following fields and options:

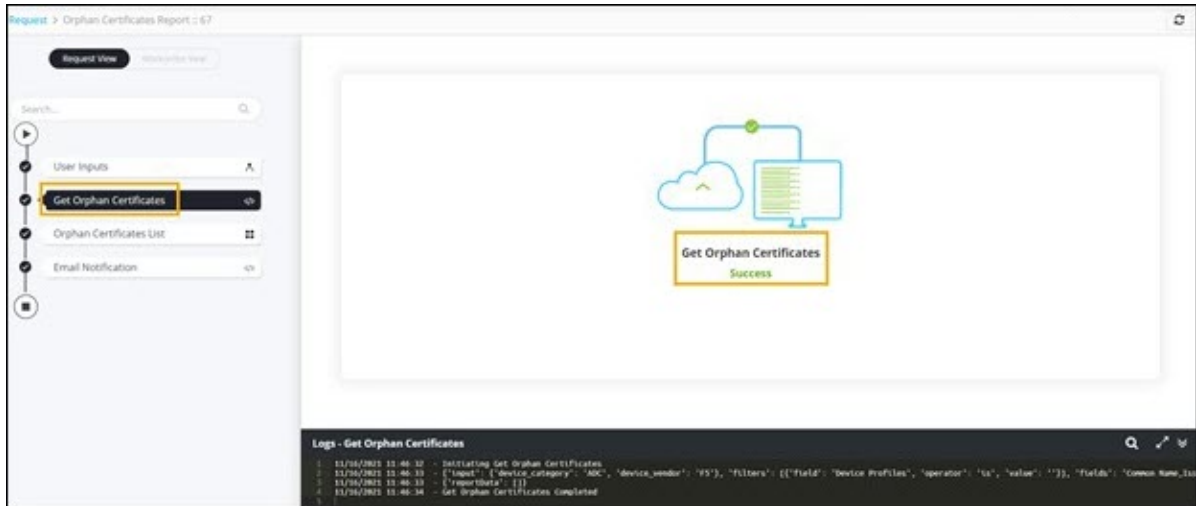
- * Email ID**: A text input field with an information icon (i) to its right.
- CC Email ID**: A text input field with an information icon (i) to its right.
- * Report Format**: A group of radio buttons with 'Email Content' selected and 'CSV Attachment' unselected.

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

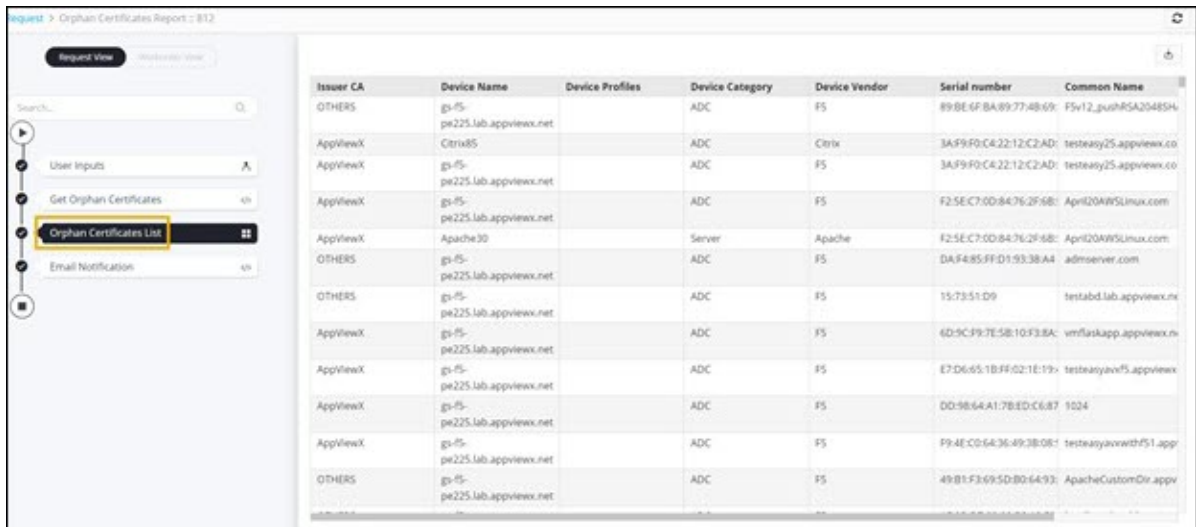
Field	Description
*Email ID	<p>Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; background-color: #e6f2ff;">  Note: The email id of the logged in user is populated automatically. </div>
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	<p>Select the required checkbox to send the report as:</p> <ul style="list-style-type: none"> • Email Content - The report will be sent as Email content. <p>or</p> <ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; background-color: #e6f2ff;">  Note: Email Content is the default selection. </div>
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.

Orphan Certificate Report for F5 Devices Inbox x  


addresssupport@appviewx.com 12:20 PM (0 minutes ago)   

 **Notification**

Request ID: 51 | Workflow Name: Orphan Certificates Report

No matching certificates found

Please do not reply as this is an auto generated email by AppViewX.

Chapter 6: Create Certificate Workflows

- [Overview](#)
- [Enroll Certificate and Download](#)
- [Certificate Provisioning with Notification](#)
- [Enroll Certificate Based on Policy | CSR Details | CSR Upload](#)
- [Create LTM SSL Profile and Enroll Certificate](#)
- [Enroll Certificate with Certificate Group and CSR Upload](#)
- [Enroll Certificate With ServiceNow](#)
- [Enroll Certificate and Push with ServiceNow](#)
- [Easy Certificate Provisioning](#)
- [Enroll Certificate with CAA Validation](#)
- [Enroll Certificate and Push](#)

Overview

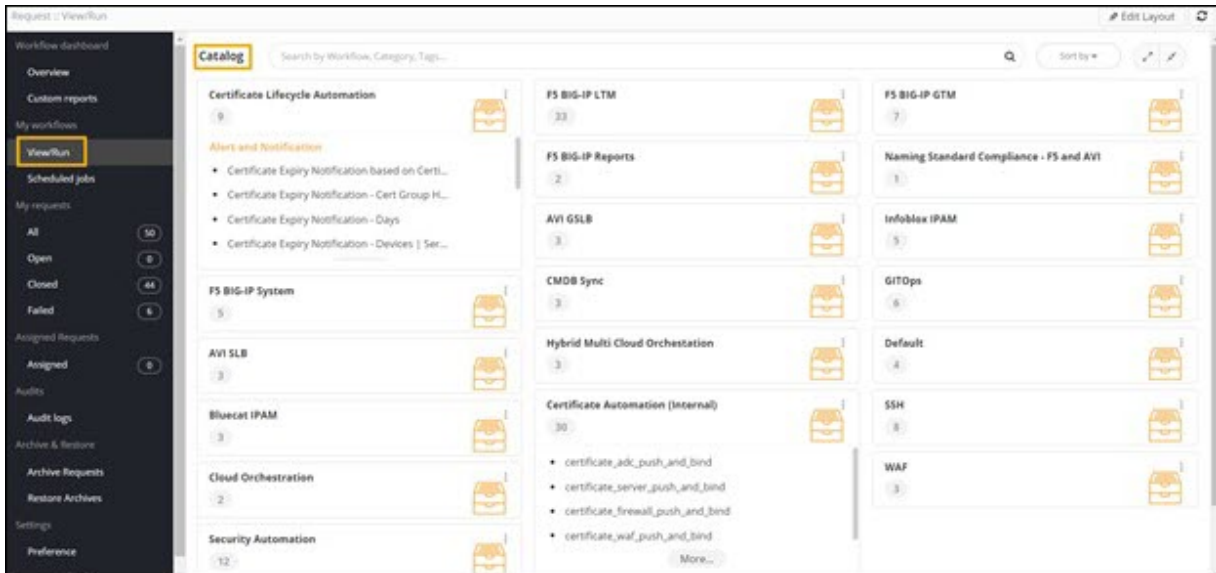
This section lists and describes the workflows that can be used to enroll certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Enrollment with Incident Automation.



Enroll Certificate and Download

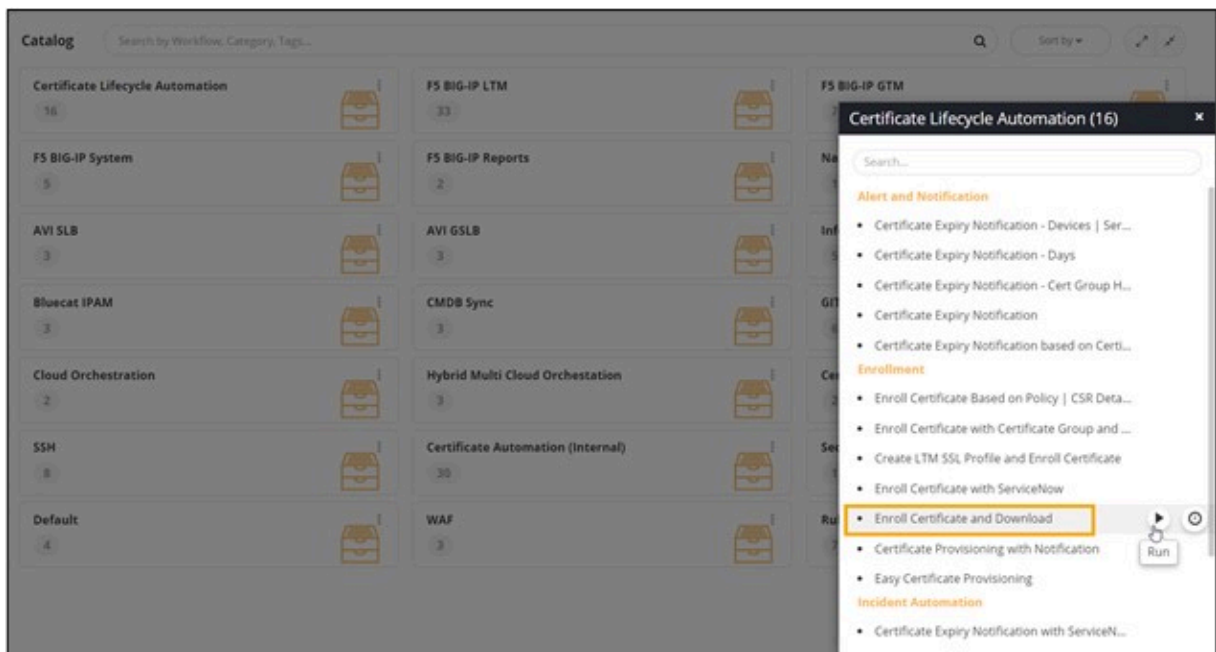
This workflow enables you to create and download certificates based on the certificate group.


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.

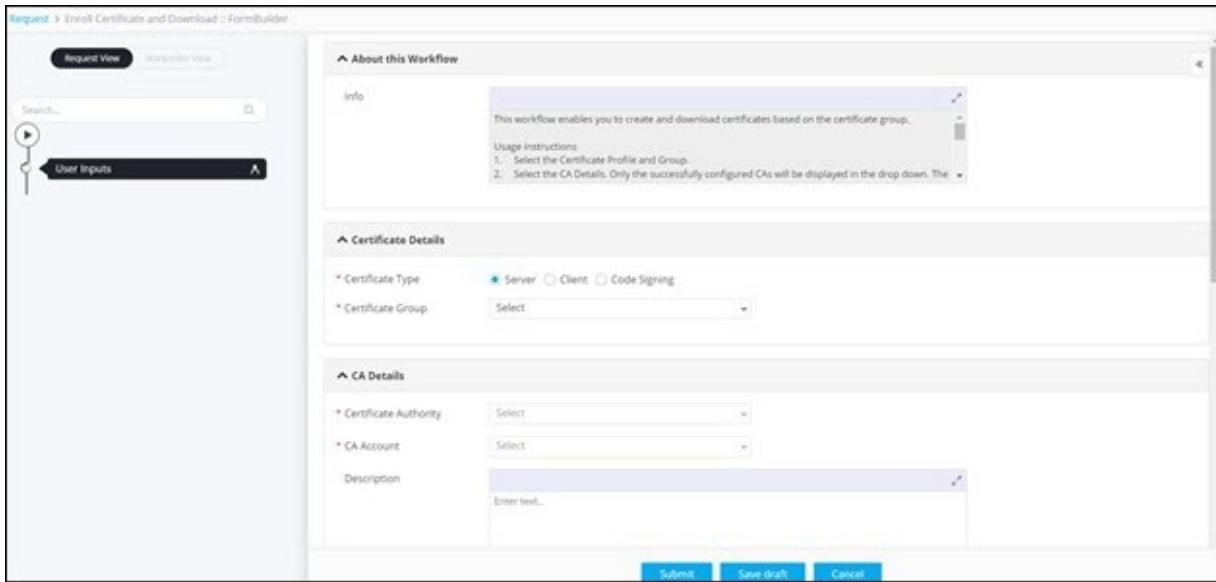


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Download** workflow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

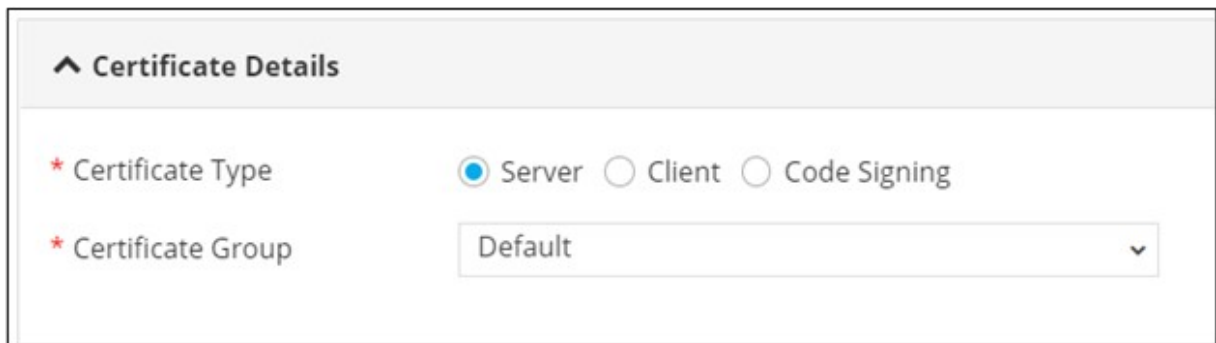


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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: <ul style="list-style-type: none"> • 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 screenshot shows the 'CA Details' section of a configuration interface. It contains the following fields:

- * Certificate Authority:** A dropdown menu with 'DigiCert' selected.
- * CA Account:** A dropdown menu with 'Select' as the placeholder.
- * Division:** A dropdown menu with 'Select' as the placeholder.
- * Cert Type:** A dropdown menu with 'Select' as the placeholder.
- Description:** A text input area with the placeholder text 'Enter text..'.




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

Field	Description
*Certificate Authority	<p>Select the Certificate Authority from the available options:</p> <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> Note: This list will be populated based on the Certificate Group selected in the Certificate Details section.</p> </div>
*CA Account	<p>Select the CA Account from the options available in the dropdown.</p> <p>Note: This field is populated based on the CA selected.</p>
*Division	<p>Select the Division from the options available in the dropdown.</p>

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.

^ CSR Parameters

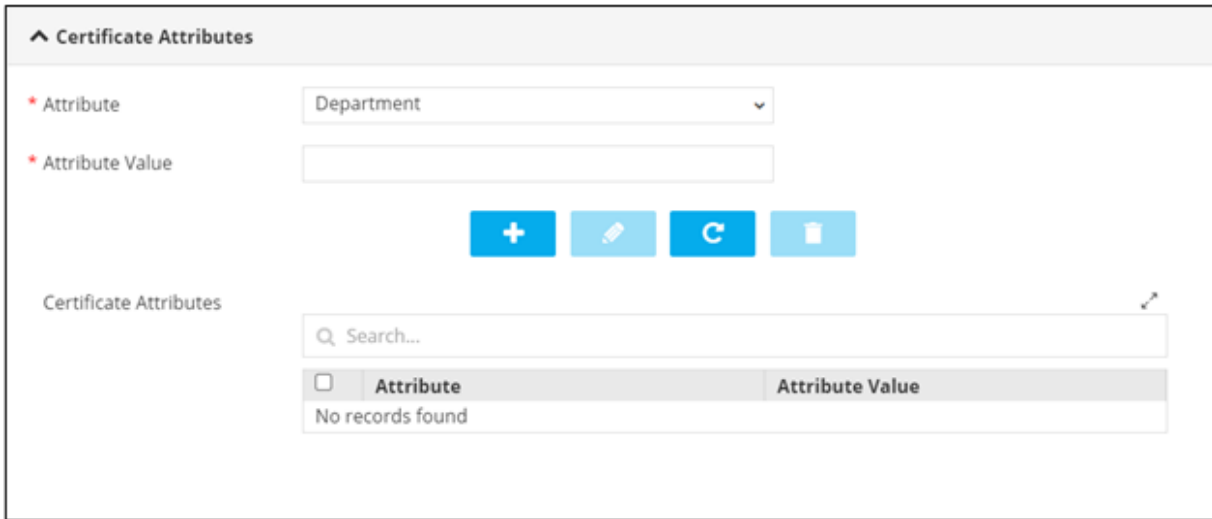
* Common Name	<input type="text" value="certenroll.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certenroll.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	
* Key Type	<input type="text" value="RSA"/>	
* Bit Length	<input type="text" value="2048"/>	
* Hash Function	<input type="text" value="SHA256"/>	






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

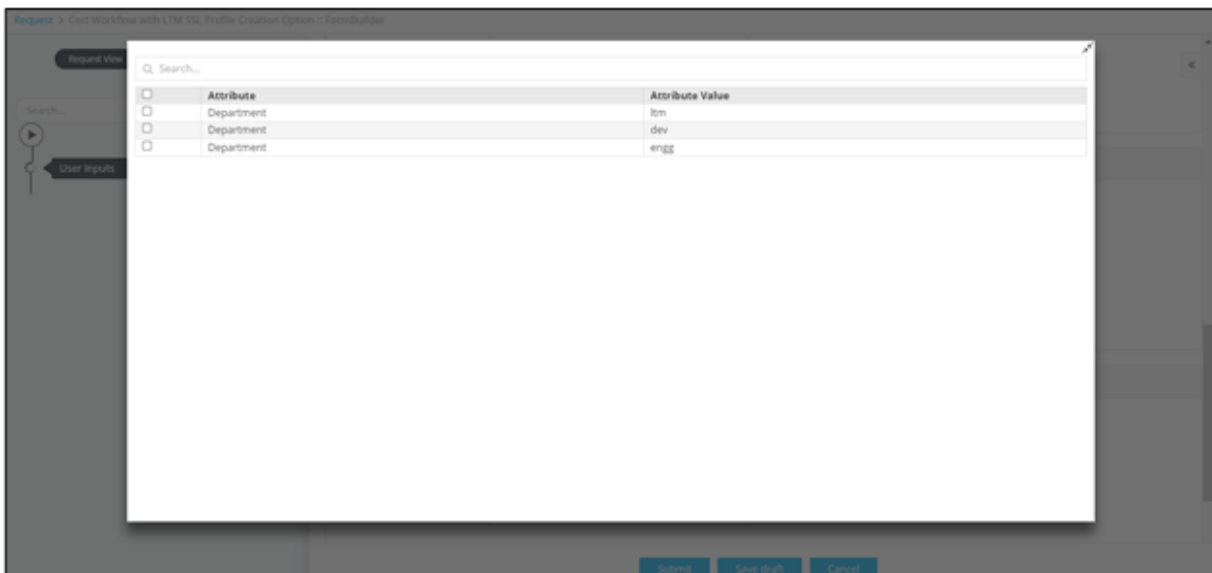
Field	Description
*Common Name	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name (SAN)	Select the SAN as either: <ul style="list-style-type: none"> • DNS • IP Address
DNS	Enter a valid DNS, if you select the DNS option in the SAN field.

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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: This field is displayed only when DigiCert is selected as the Certificate Authority. </div>
Email Address	Enter the email address.
*Validity Unit	Select the validity unit as: <ul style="list-style-type: none"> • 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.

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ Notifications

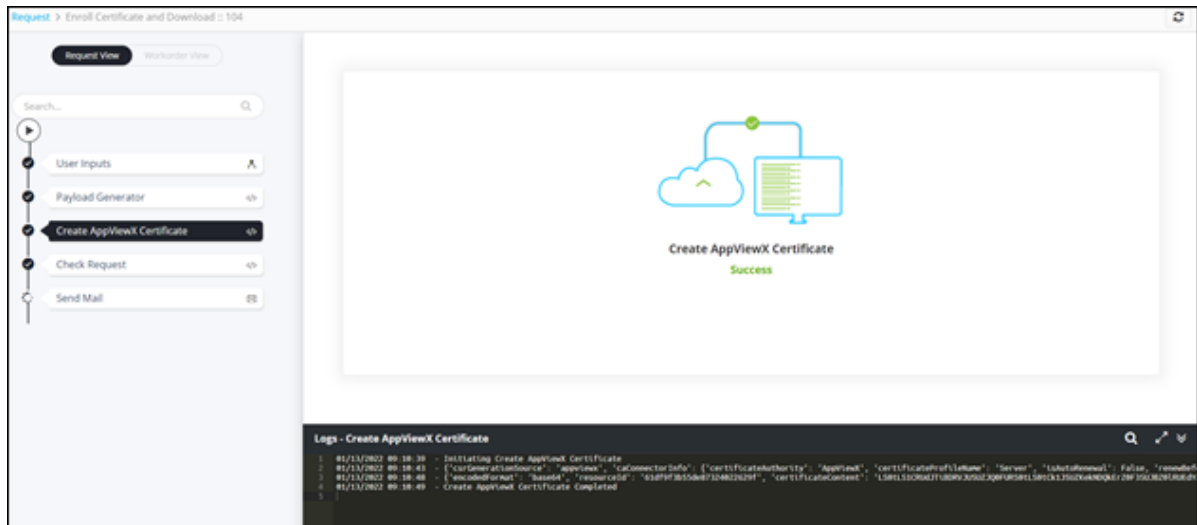
* Email ID ⓘ



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**.

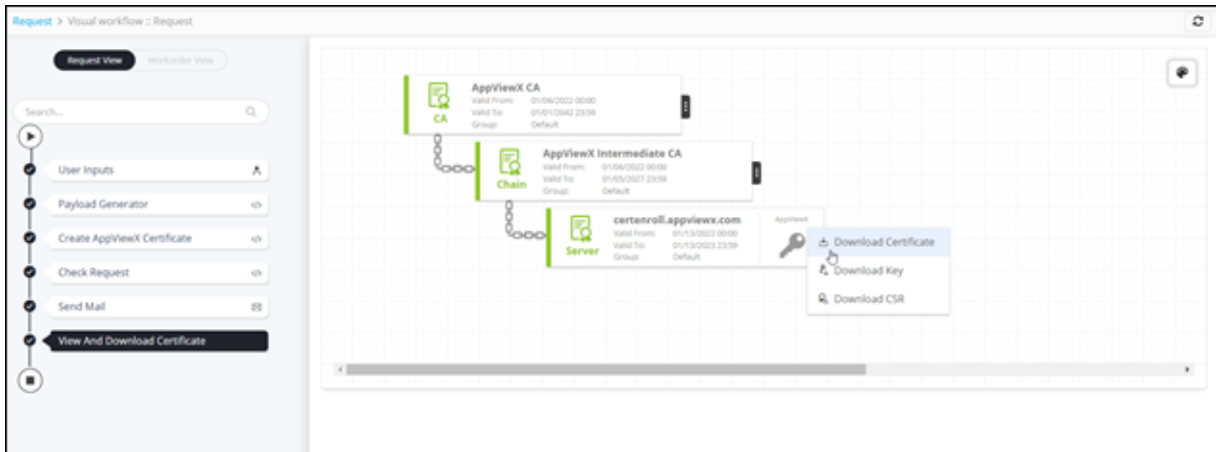
- Certificate created successfully.



- 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.

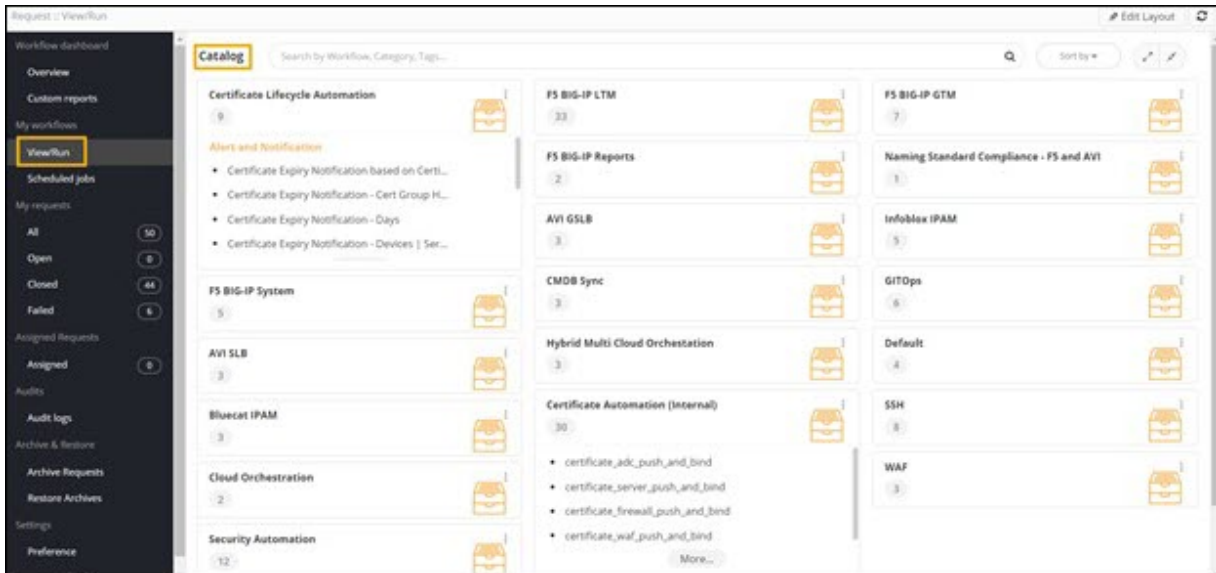




Certificate Provisioning with Notification

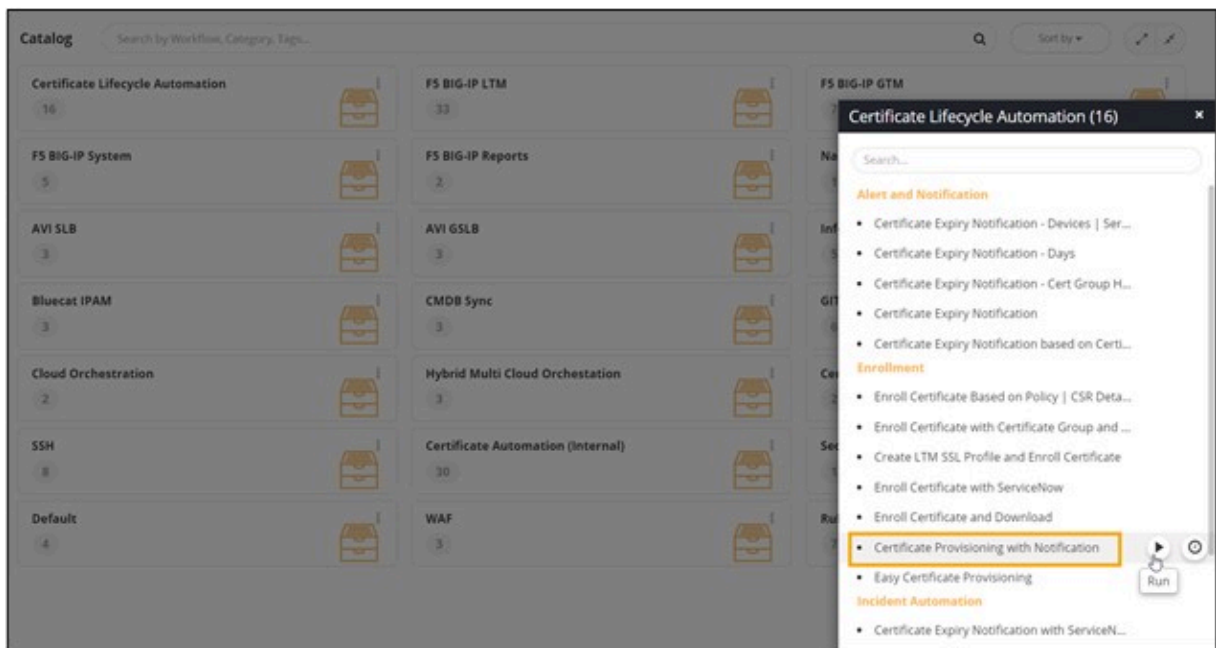
This workflow allows you to create a certificate based on the certificate group and the policy associated with it, and push to a device available in the instance. Email approval is required for certificate creation as well as pushing it to the device. Once approved, the logged in user will receive an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

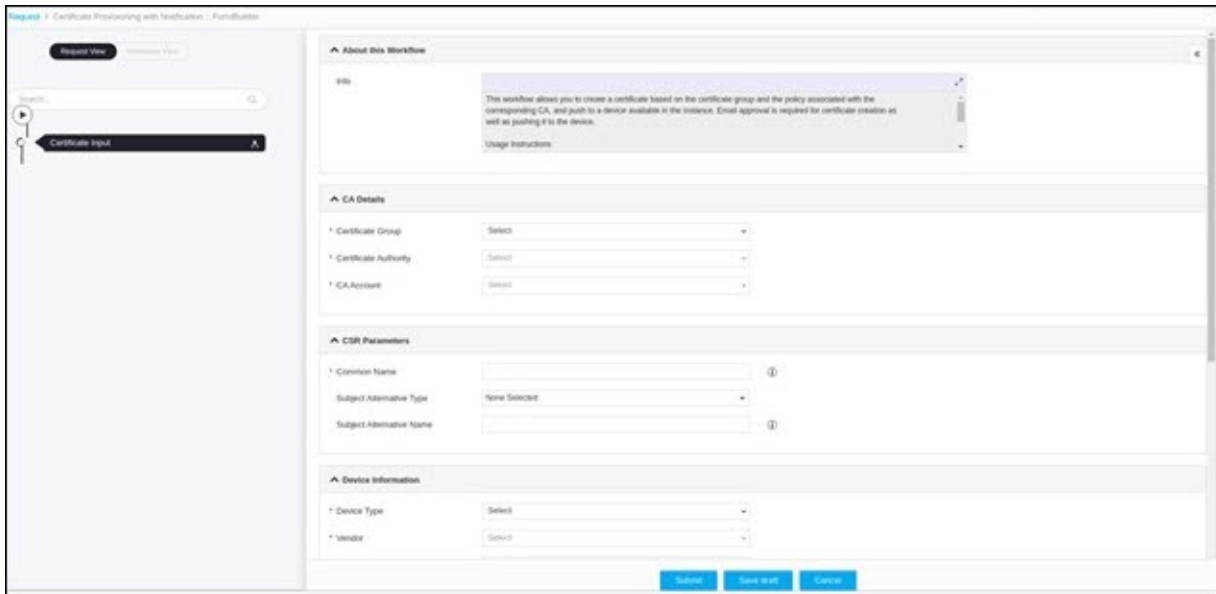


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click  .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Certificate Provisioning with Notification**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

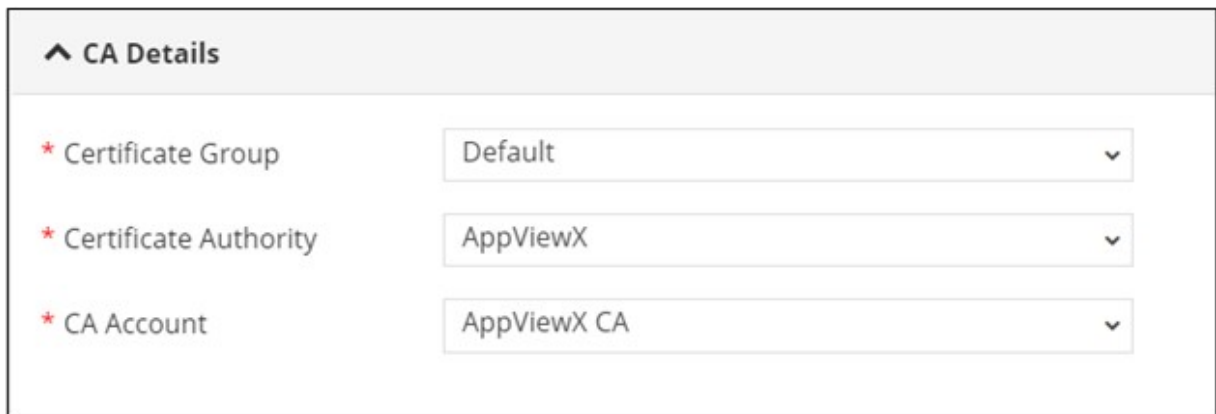


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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: <ul style="list-style-type: none"> • DigiCert • Ebtrust • EJBCA


Field	Description
	<ul style="list-style-type: none"> • Microsoft Enterprise • AppViewX <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the selected Certificate Group. </div>
CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the CA selected . </div>
All asterisk (*) marked fields are mandatory.	

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

^ CSR Parameters

* Common Name 

Subject Alternative Type




Subject Alternative Name 



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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #007bff; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: The vendor list is populated based on the Device Type selected. </div>
* Device	Select the Device from the options available in the dropdown. <div style="border: 1px solid #007bff; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: The device list is populated based on the Vendor selected. </div>
Linux Actions	Select the Linux Action from the options available in the dropdown. <div style="border: 1px solid #007bff; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when you select Linux Server in the Vendor field. </div>
* 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.

Device Information

* Device Type:

* Vendor:

* Device:

* Linux Actions:


* Profiles/Application:

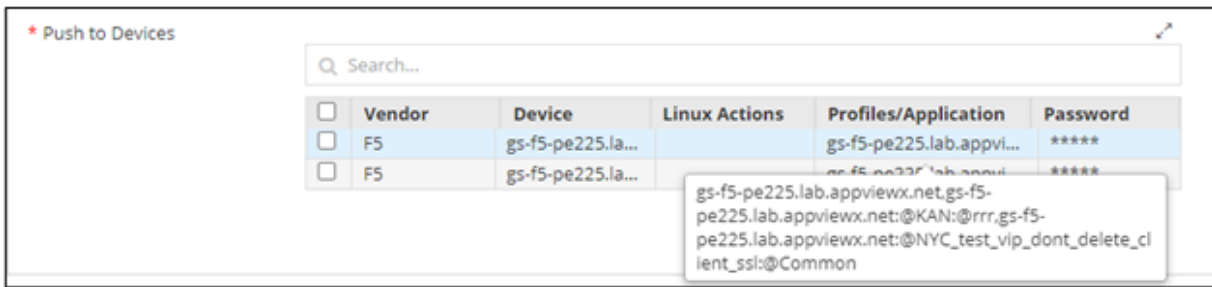
* KDB Password:





* Push to Devices

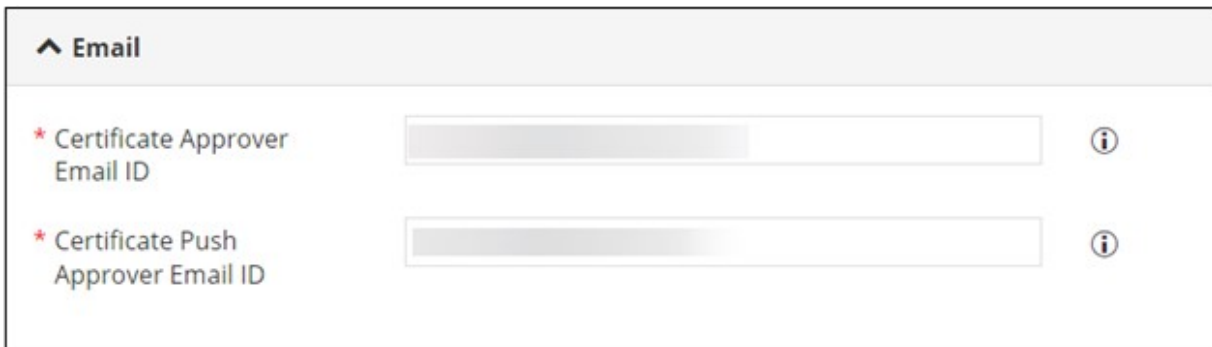
Search...

<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****

 **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.



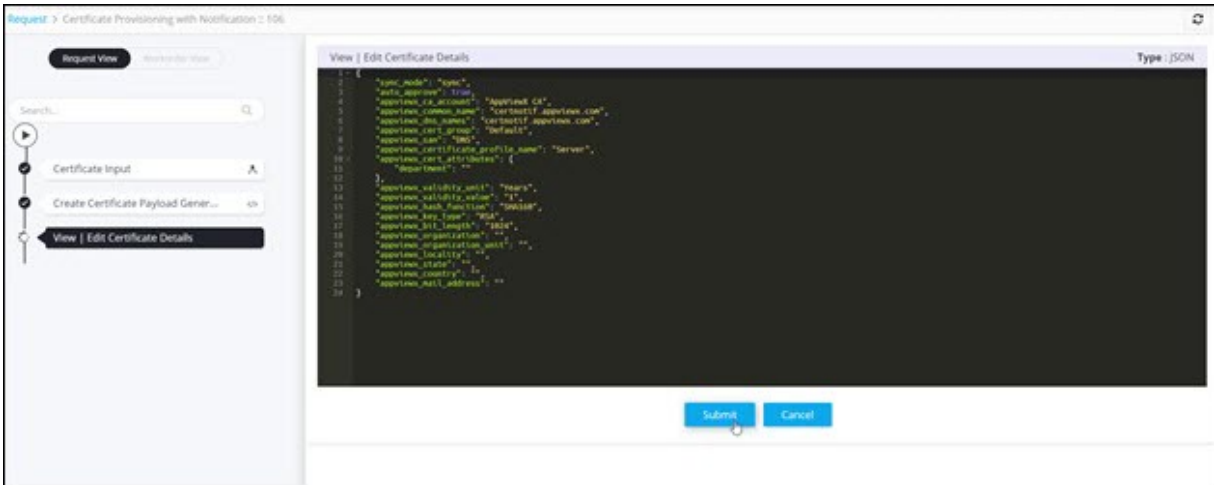
The following table describes the field information under the **Email** section:

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.	

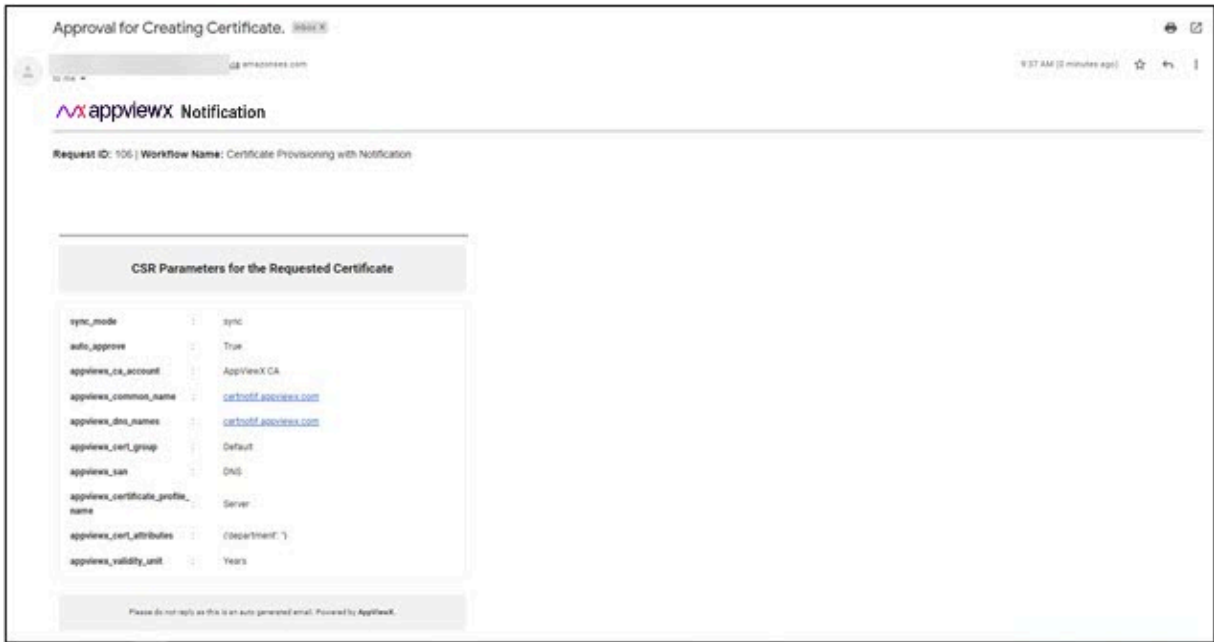
15. Click **Submit**.

The workflow is executed.

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



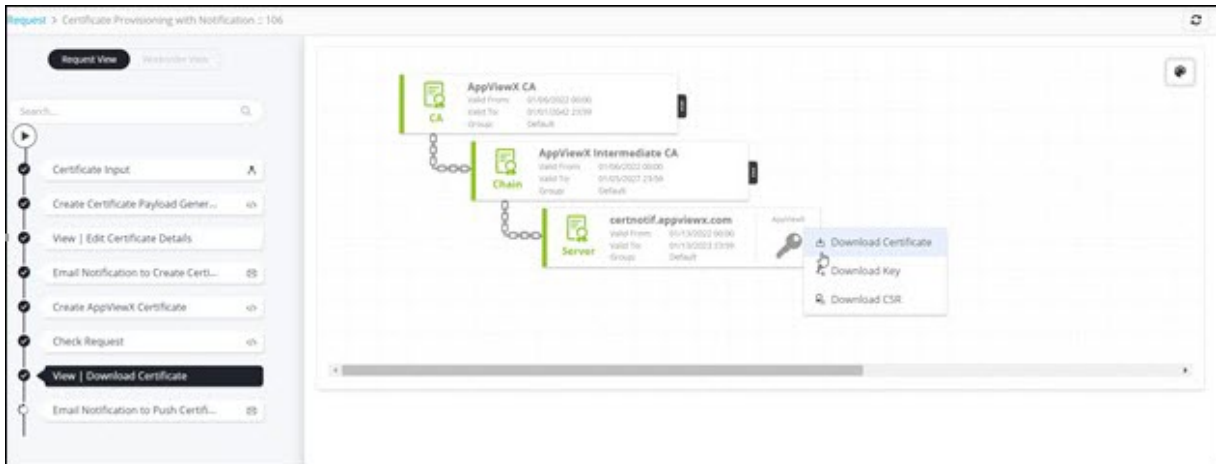
Email notification for Create Certificate approval received.



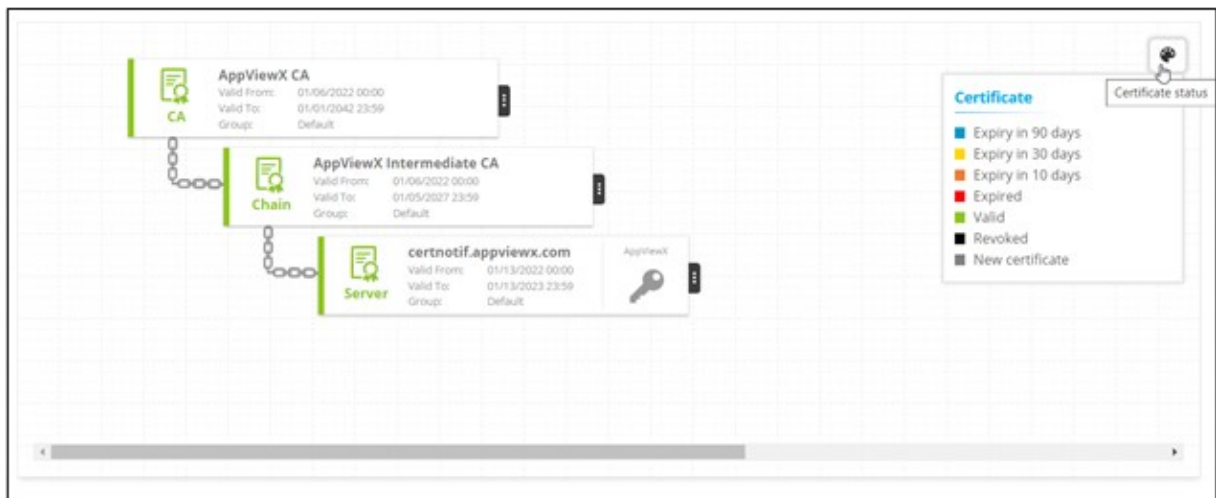
17. Click **Approve** or **Reject** in the **Approval for Creating Certificate** email.

Certificate is created after the approver clicks **Approve**.

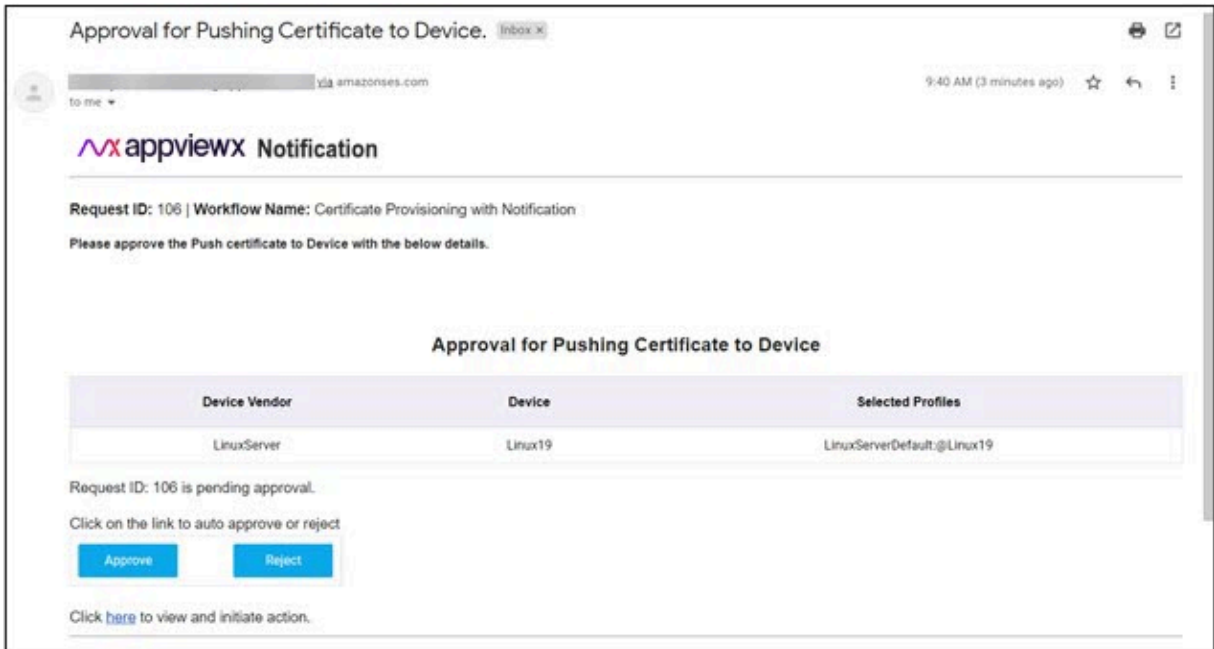
18. To download the certificate, at the **View | Download Certificate** stage, hover your mouse over , and from the options displayed, click **Download Certificate**.



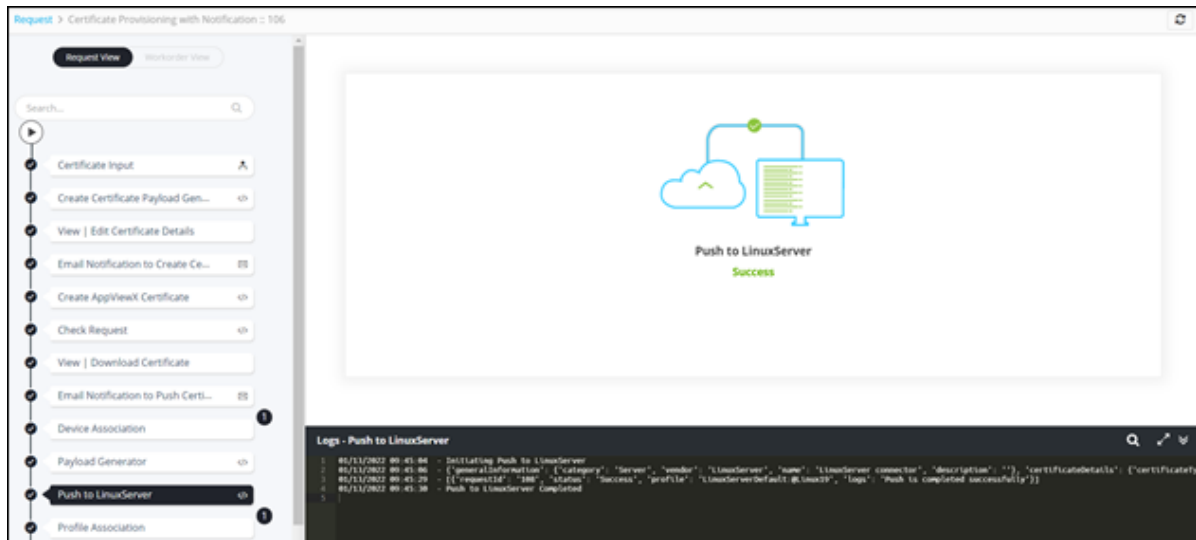
19. Hover your mouse over  to view the Certificate status.



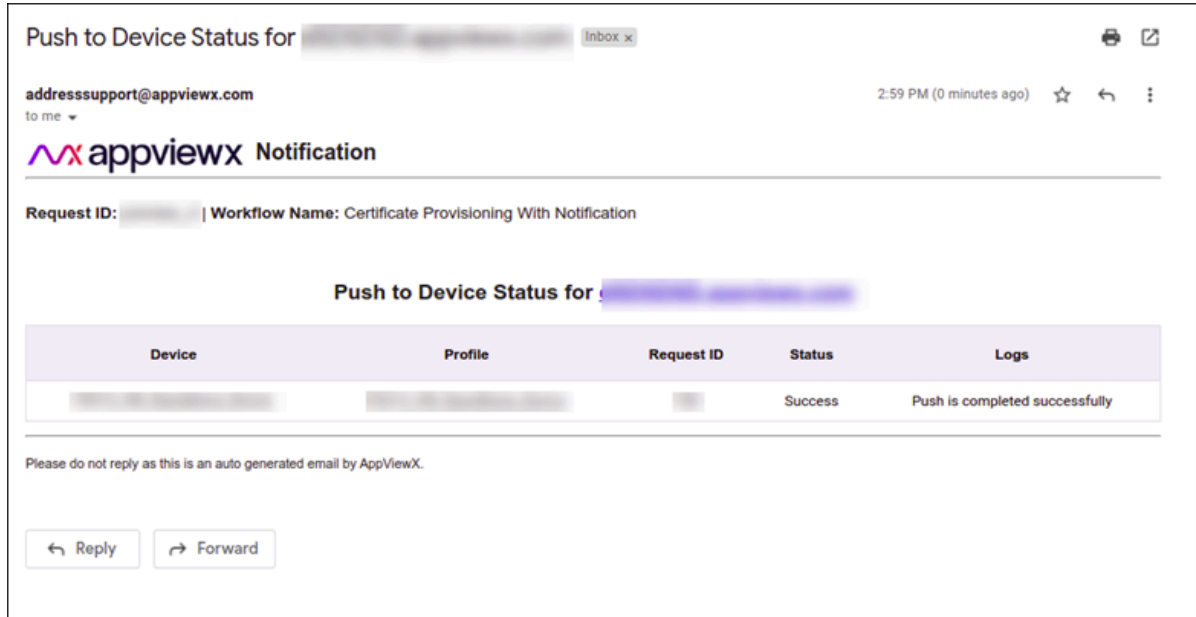
20. Click **Approve** or **Reject** in the **Approval for Pushing Certificate to Device** email.



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



- Email notification received.

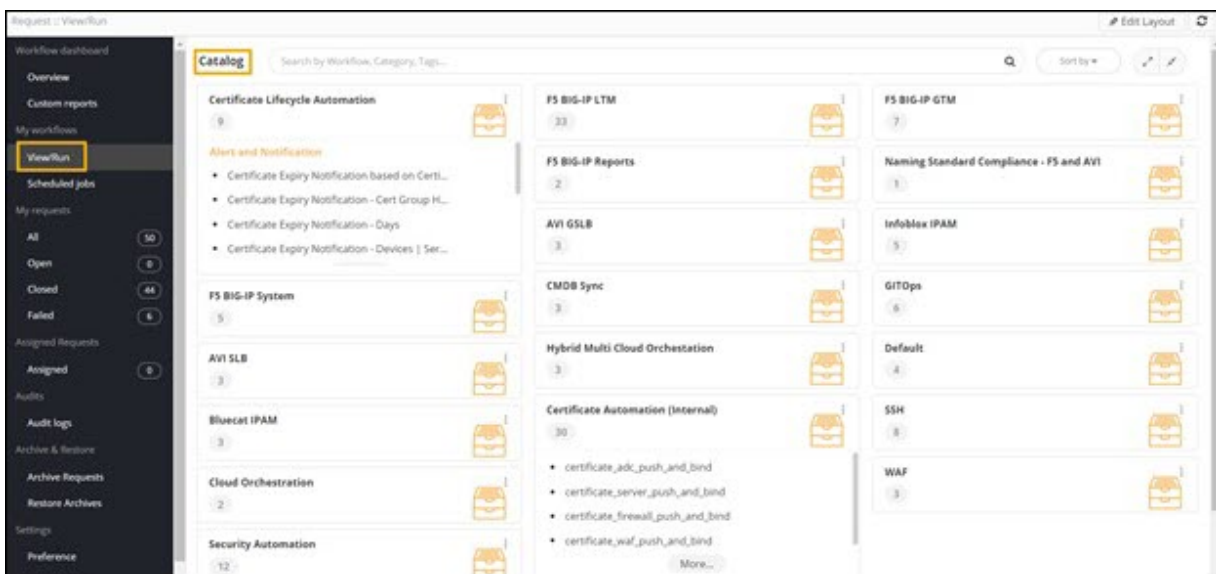




Enroll Certificate Based on Policy | CSR Details | CSR Upload

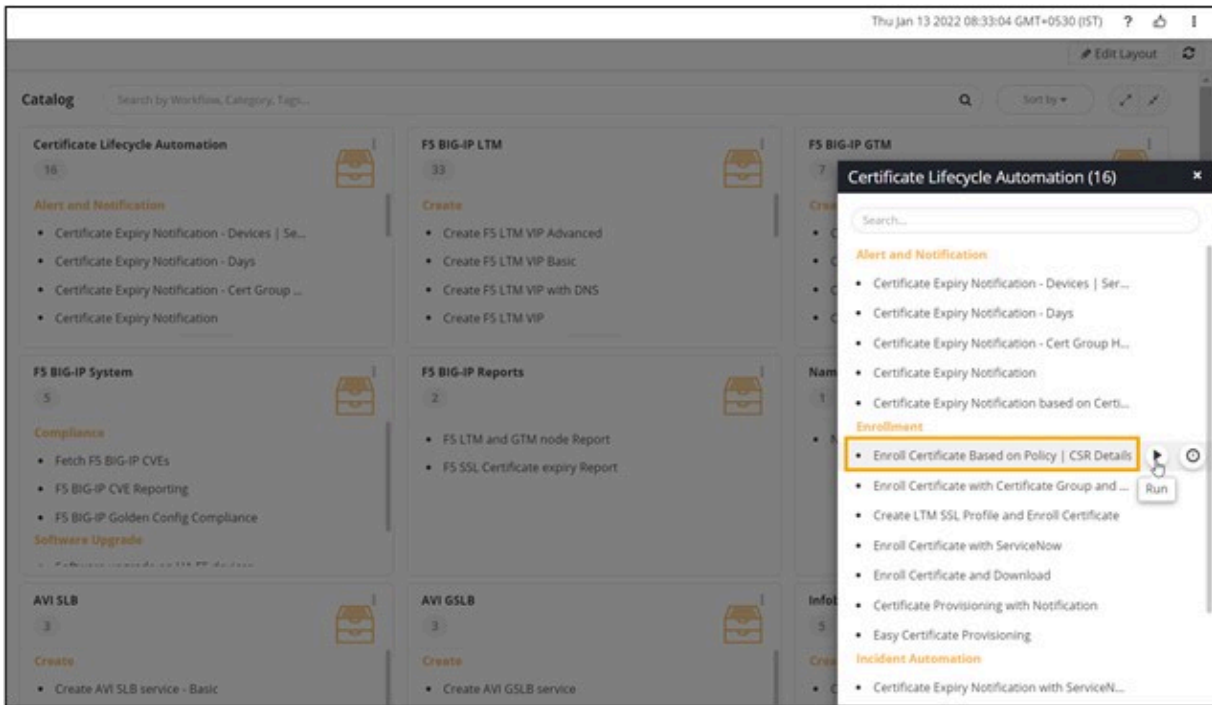
This workflow allows you to create a certificate using three input methods - Manual, Policy Based, and Upload CSR.


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.

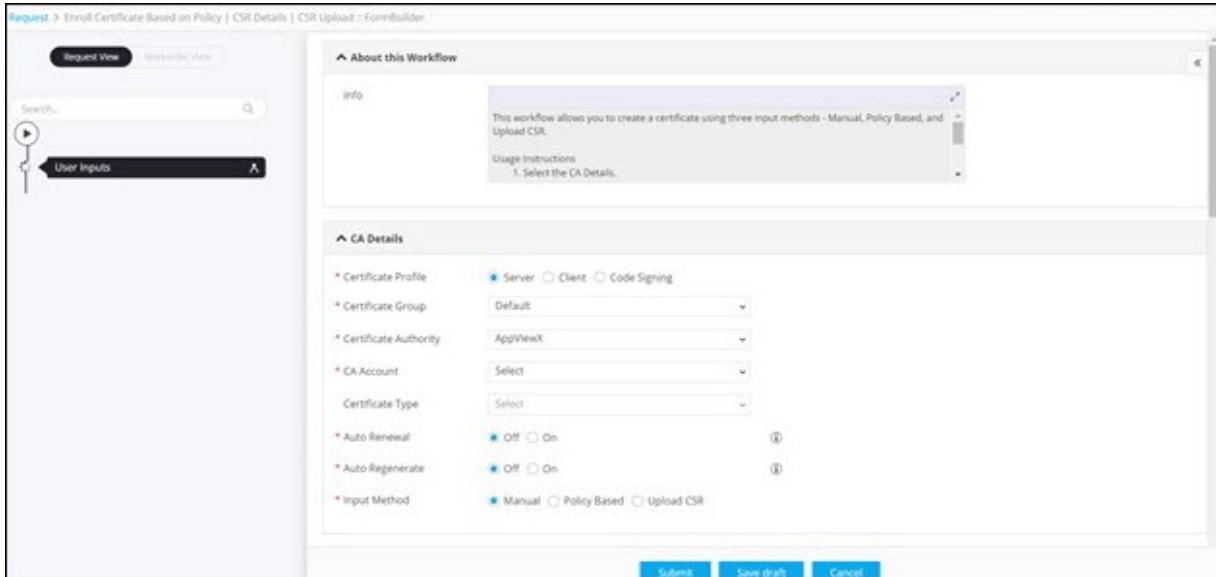


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate Based on Policy | CSR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

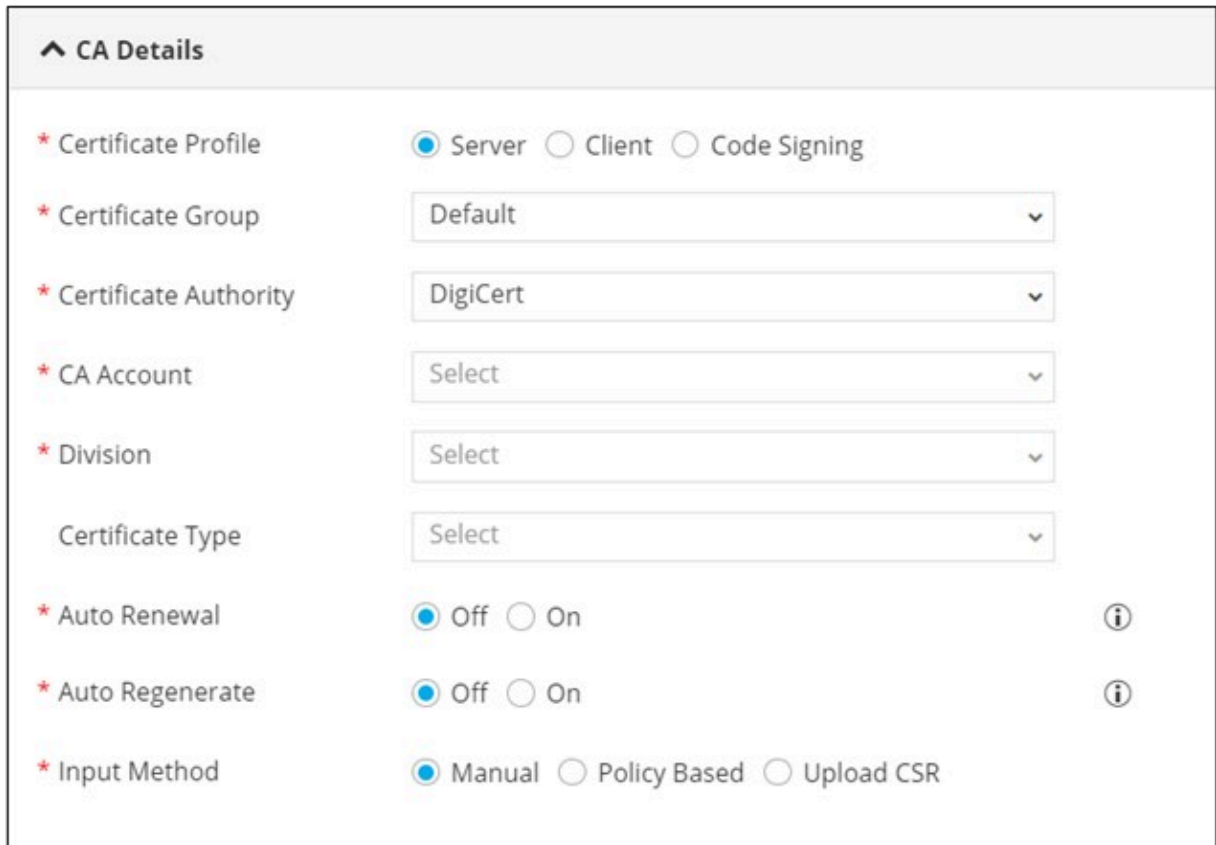


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.






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: <ul style="list-style-type: none"> • Server • Client • Code Signing <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Server is the default selection. </div>
*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: <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the Certificate Group selected. </div>
*CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the Certificate Authority selected. </div>
*Division	Select the Division from the options available in the dropdown. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when DigiCert is selected as the CA. </div>
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 . <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Default selection is set to Off. </div>

Field	Description
Renew Before (Days)	<p>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.</p> <p> Note: This field is displayed only when the Auto Renewal field is enabled.</p>
*Auto Regenerate	<p>Select the required radio button to enable/disable Auto Regenerate.</p> <p> Note: Default selection is set to Off.</p>
Start Regenerating (Days)	<p>Enter the number of days in the Start Regenerating (days) field.</p> <p> Note: This field is displayed only when the Auto Regenerate field is enabled.</p>
*Input Method	<p>Select the required Input Method. The options available are:</p> <ul style="list-style-type: none"> • 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. <p> Note: Manual is the default selection.</p>
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.

^ CSR Parameters		
* Common Name	<input type="text" value="certadvmanual.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certadvmanual.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
Challenge Password	
* Hash Function	SHA160
* Key Type	RSA
* Bit Length	Select

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: <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>
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.

^ Certificate Attributes

* Attribute

* Attribute Value


+
✎
↻
🗑

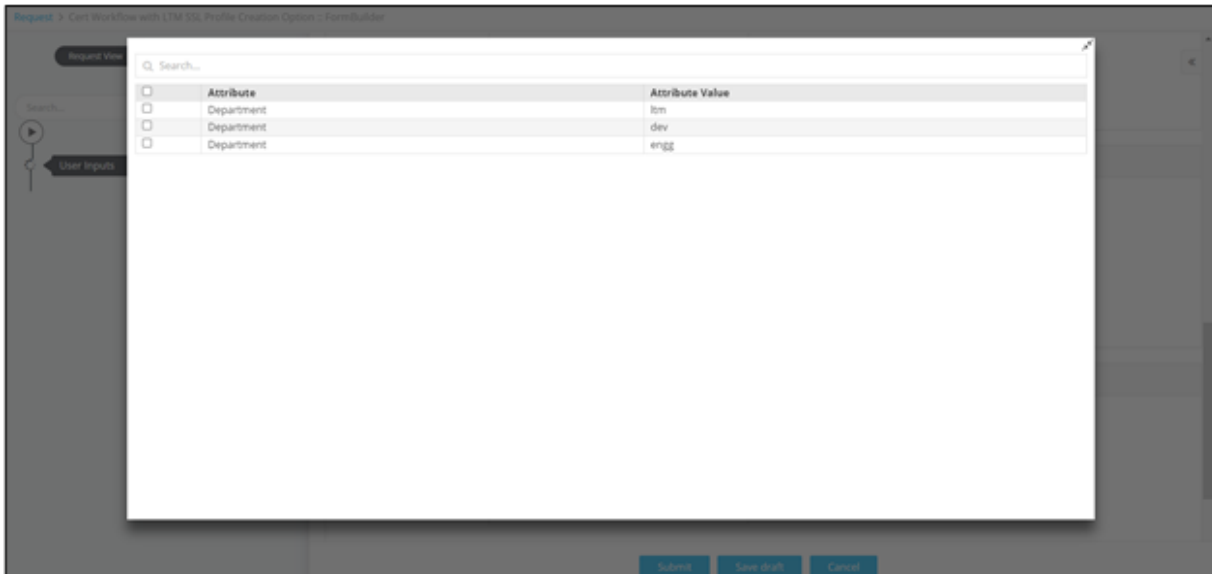
Certificate Attributes

🔍 Search...

	Attribute	Attribute Value
❑	Attribute	Attribute Value
No records found		

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.

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ Notifications

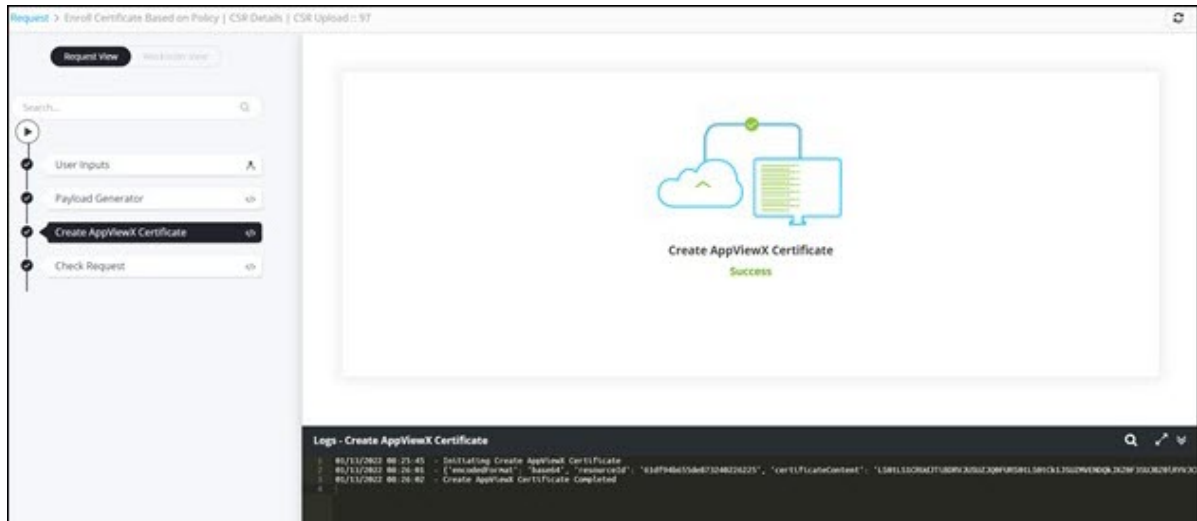
* Email ID ⓘ



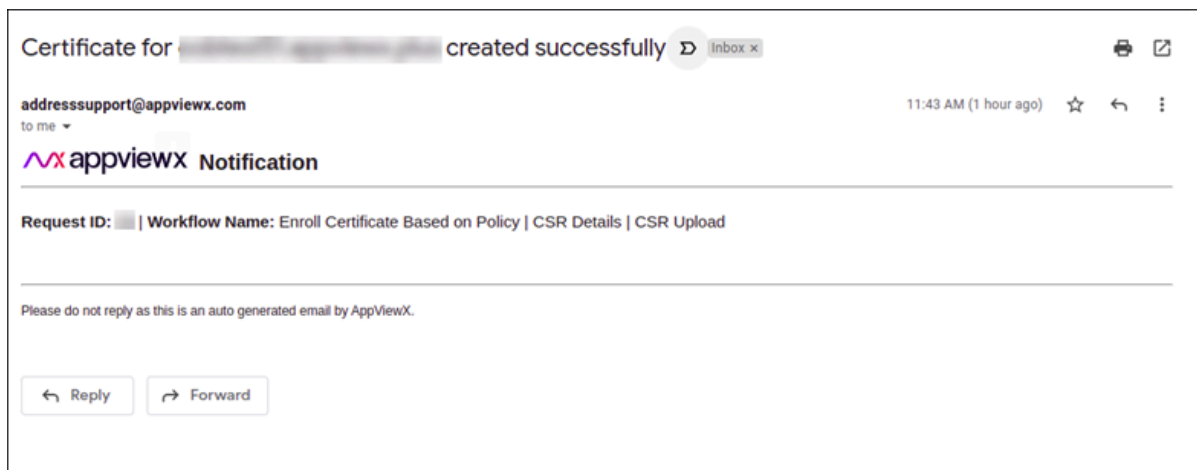
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

12. Click **Submit**.

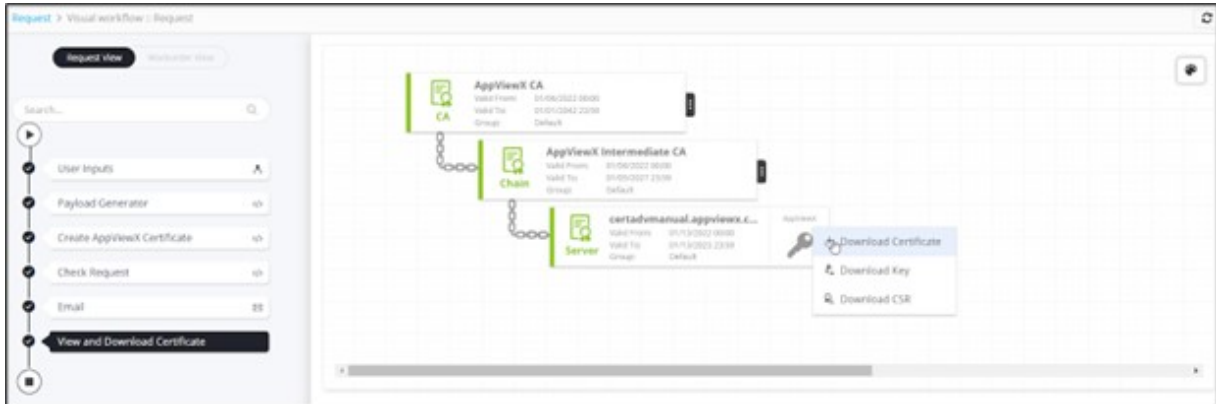
- AppViewX certificate created.



- 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**.

^ CSR Parameters		
* Common Name	<input type="text" value="certadvpolicy.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certadvpolicy.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text" value="Product Engineering"/>	
Locality	<input type="text" value="San Diego"/>	
State	<input type="text" value="Texas"/>	
Country	<input type="text" value="US"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
Challenge Password	
* Hash Function	SHA160
* Key Type	RSA
* Bit Length	Select



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.

^ Certificate Attributes

* Attribute: Department



* Attribute Value:




+ ✎ C 🗑

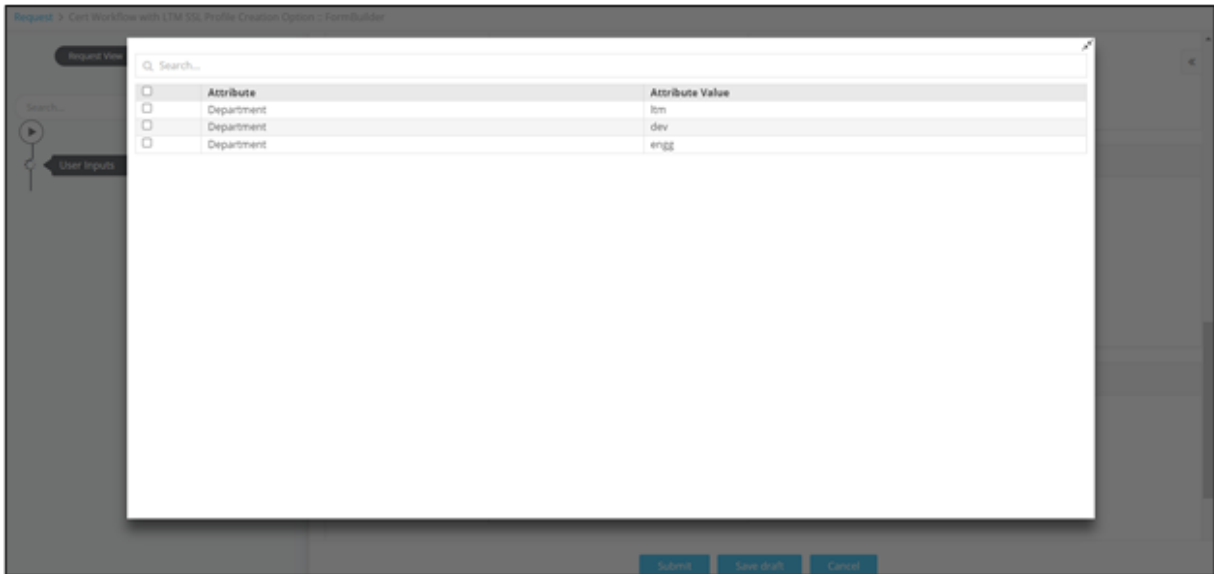
Certificate Attributes

🔍 Search...

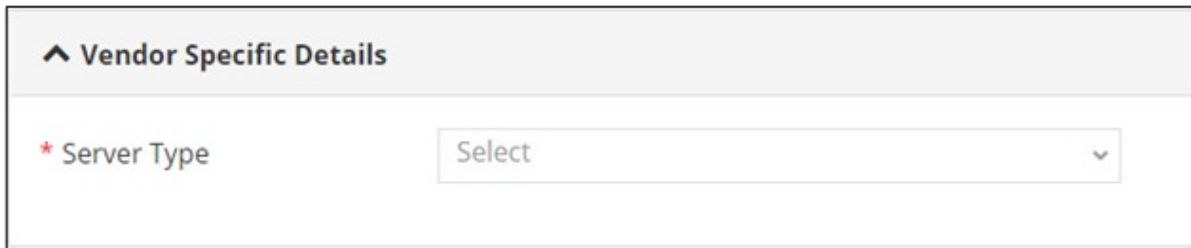
Attribute	Attribute Value
No records found	

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.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name


* Certificate Profile Name



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.

^ Notifications

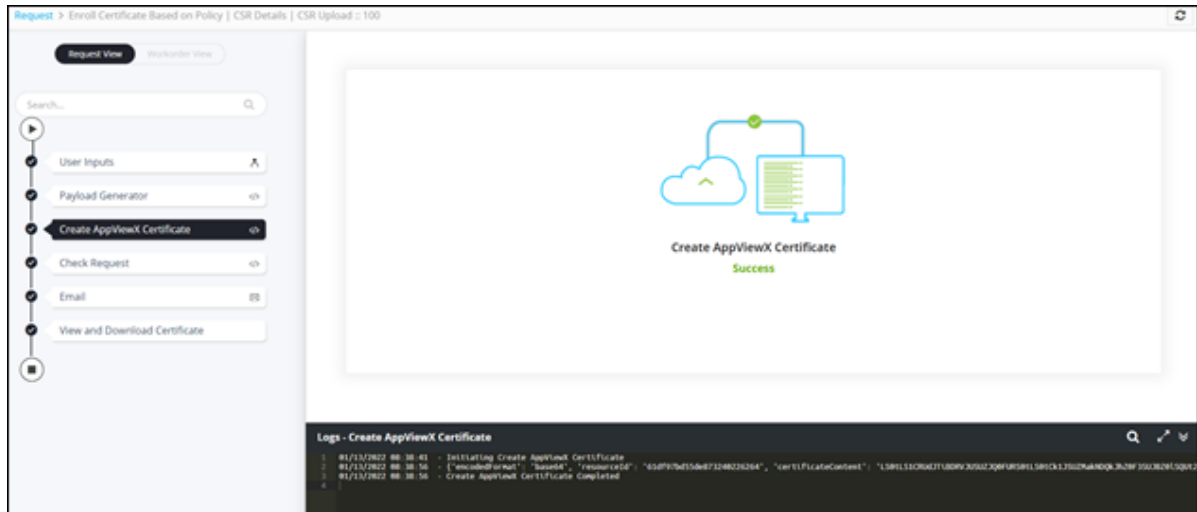
* Email ID 



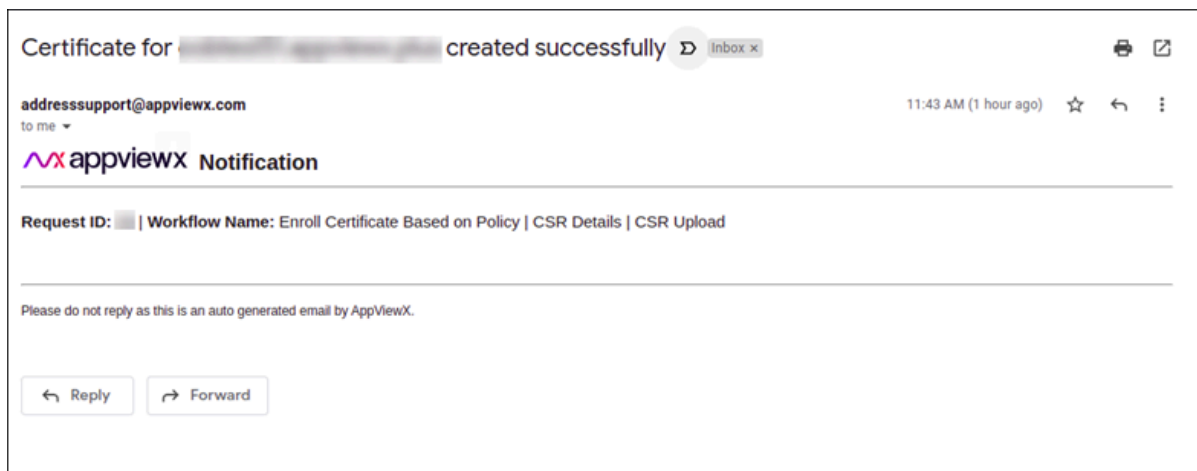
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

12. Click **Submit**.

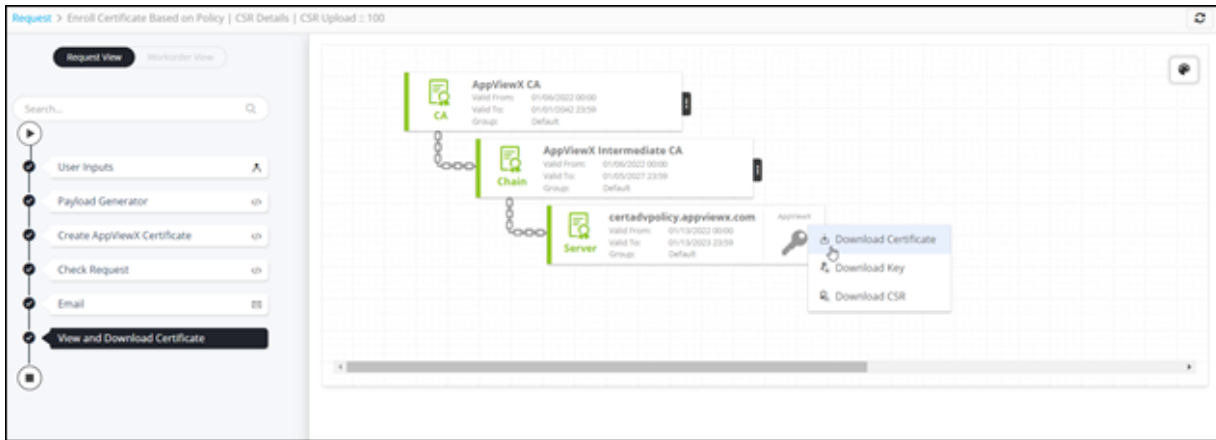
- AppViewX certificate created.



- Email notification received.



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




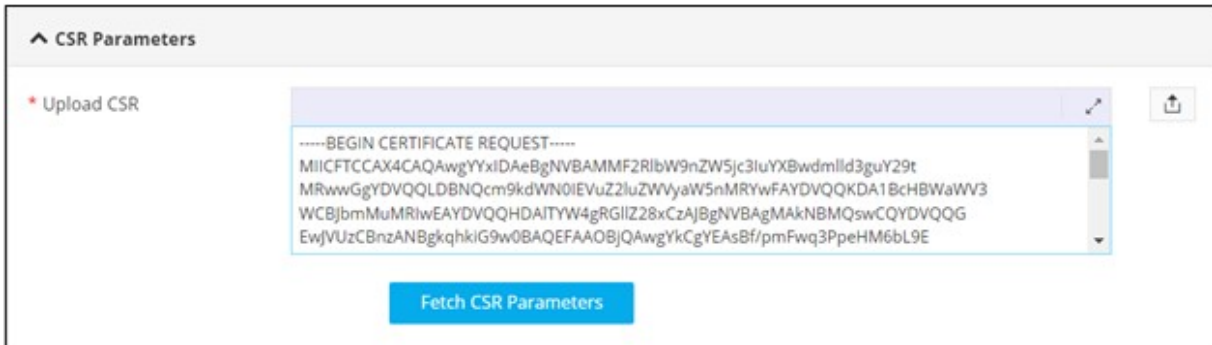
14. Hover your mouse over  to view the **Certificate status**.



Upload CSR

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

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



CSR Parameters

Upload CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIICFTCCAX4CAQAwgYYxiDAeBgNVBAMMF2RibW9nZW5jc3luYXBwdmllid3guY29t
MRwwGgYDVQQQLDBNQcm9kdWN0IEVuz2luZWVyaW5nMRYwFAYDVQQKDA1BcHBWYWV3
WCBJbmMuMRlwEAYDVQQQHDAITYW4gRGlIZ28xCzAJBgNVBAGMAkNBMQswCQYDVQQG
EwjVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA5Bf/pmFwq3PpeHM6bL9E
```

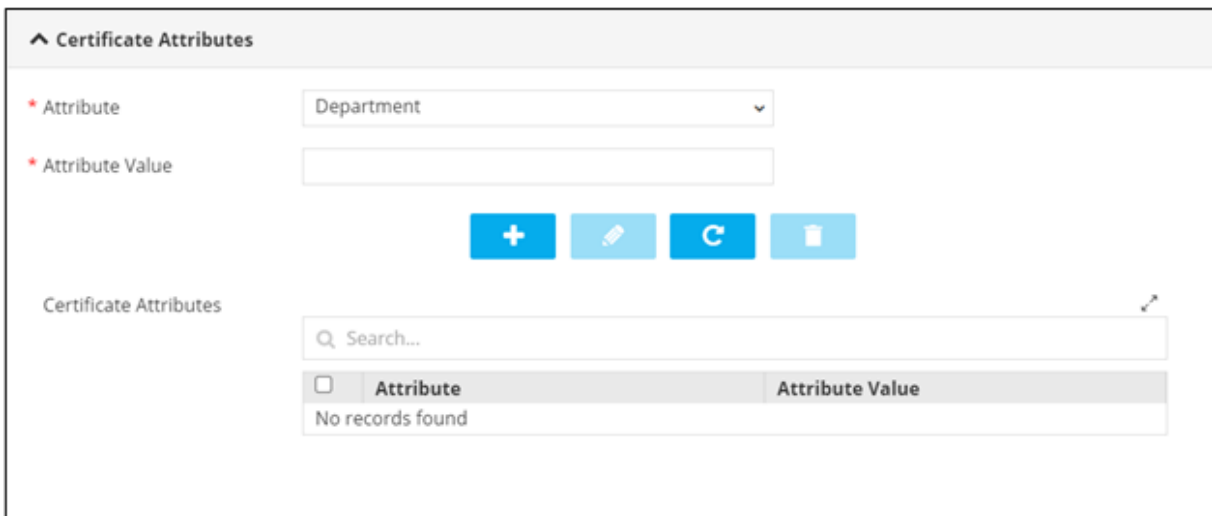
Fetch CSR Parameters

- 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.

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



Certificate Attributes

Attribute: Department





Attribute Value:


+ | Edit | Refresh | Delete

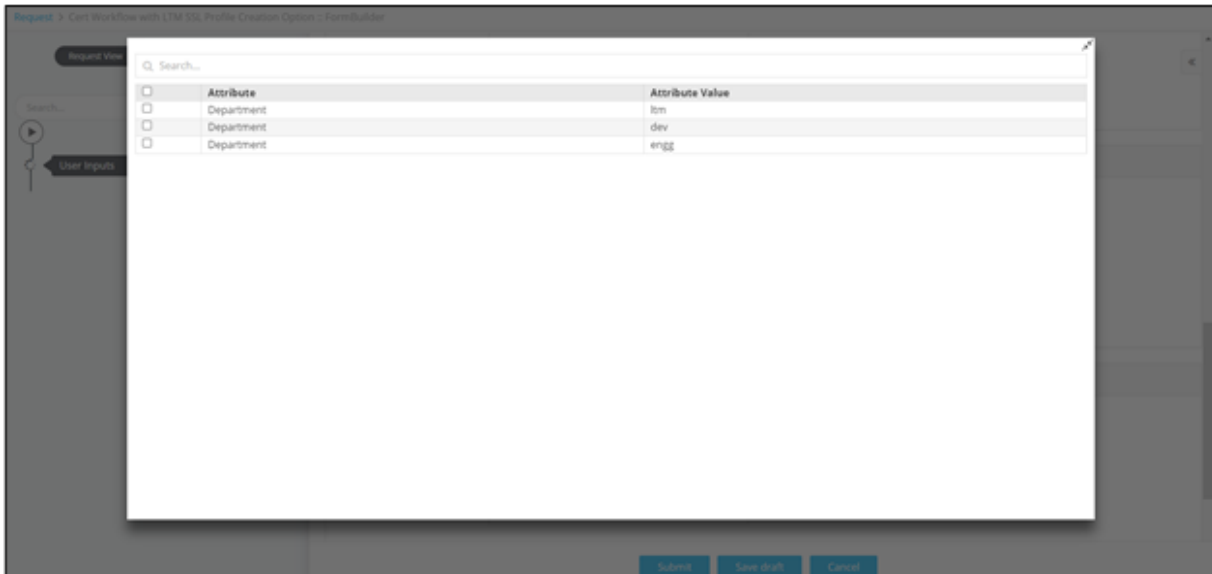
Certificate Attributes

Search...

Attribute	Attribute Value
No records found	

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

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ Notifications

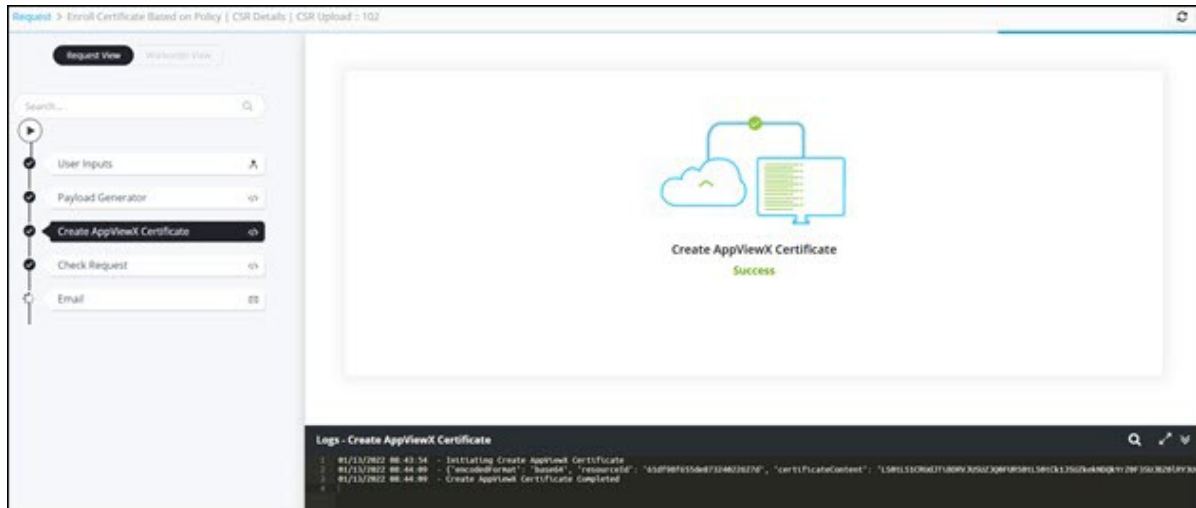
* Email ID ⓘ



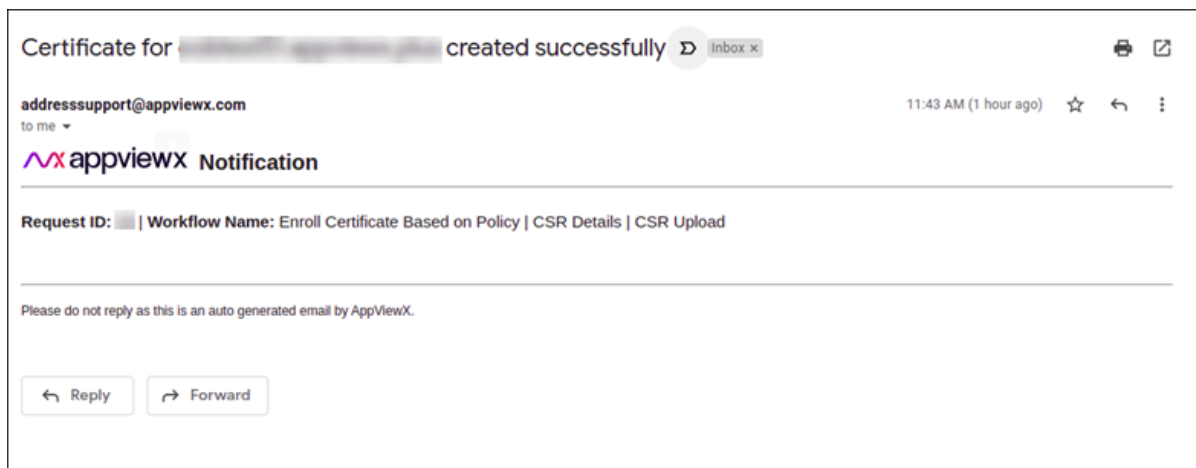
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.

- AppViewX certificate created.



- Email notification received.



- 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**.

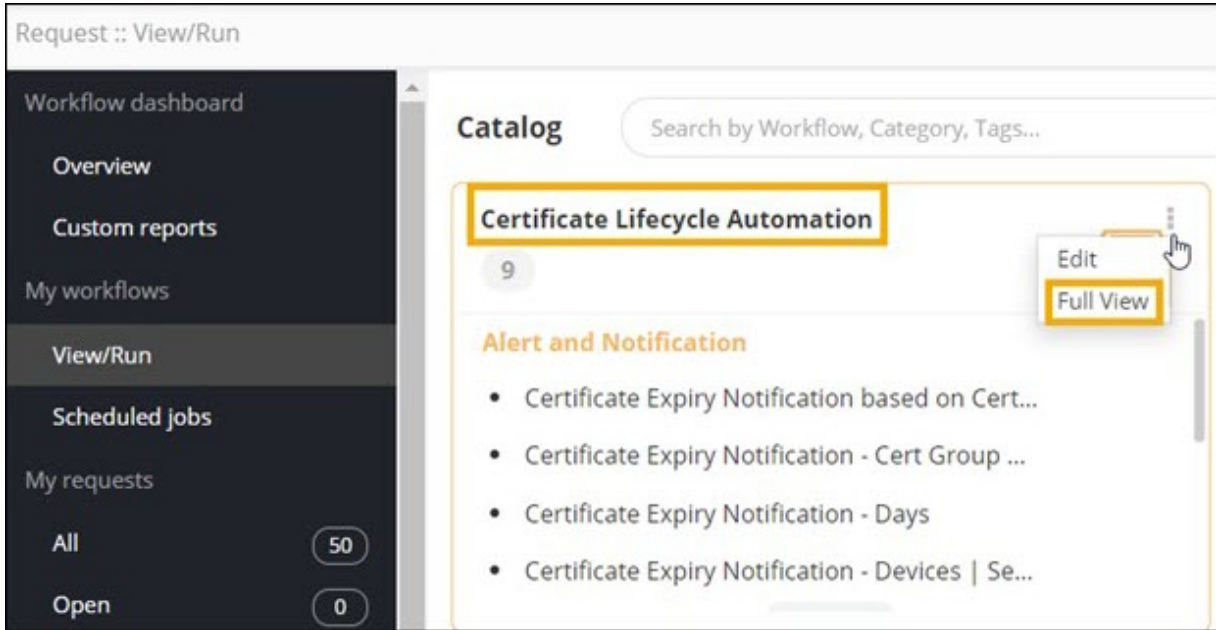




Create LTM SSL Profile and Enroll Certificate

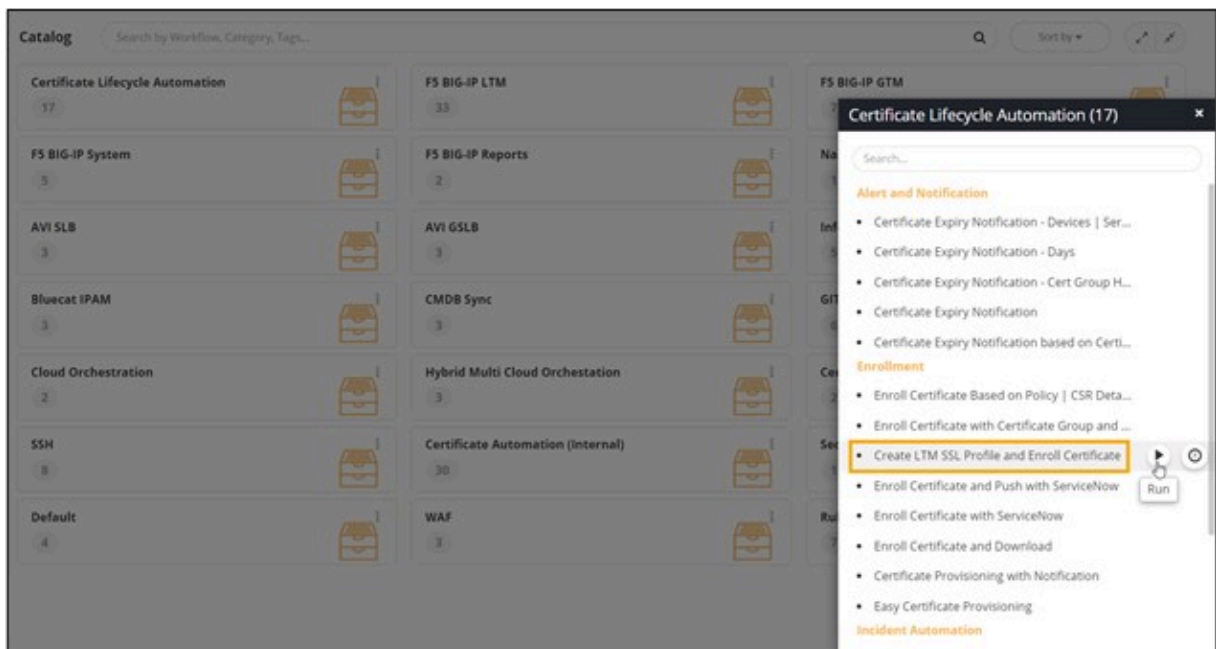
This workflow allows you to create individual server certificates along with LTM SSL profile creation based on the selected certificate group.

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.

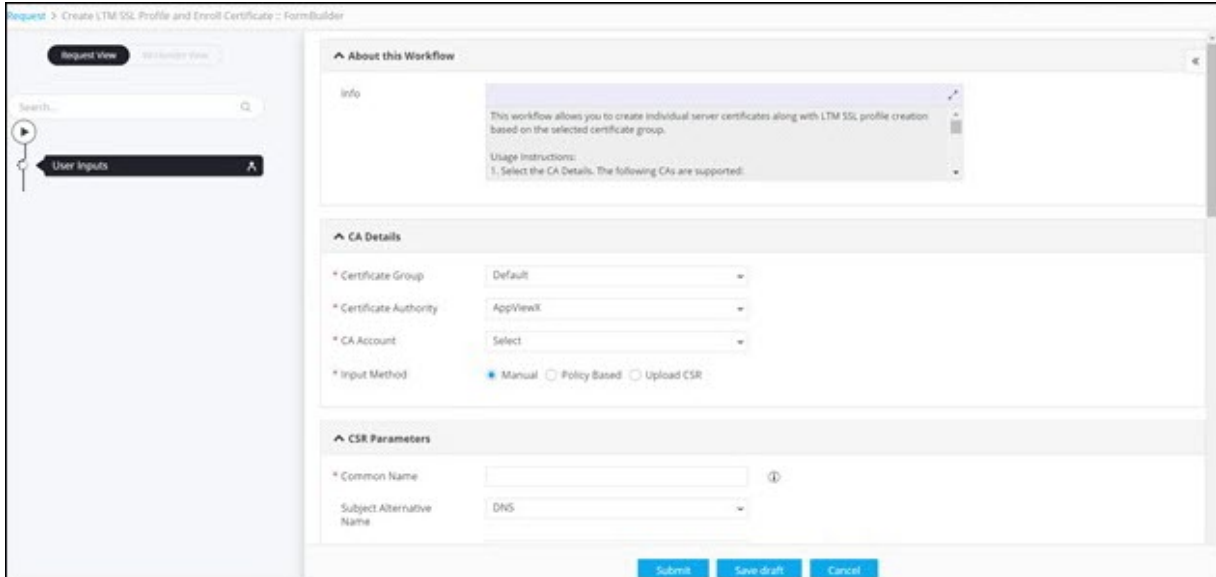


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Create LTM SSL Profile and Enroll Certificate**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







i **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: <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: The Certificate Authority field is populated based on the selected Certificate Group. </div>
*CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: The CA Account field is populated based on the selected Certificate Authority. </div>
*Division	Select the Division from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field is displayed only when DigiCert is selected as the CA. </div>
*Cert Type	Select the Cert Type from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field is displayed only when DigiCert or Entrust are selected as the CA. </div>
*Input Method	Select the required Input Method . The options available are: <ul style="list-style-type: none"> • 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](#)
- [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.

^ CSR Parameters

* Common Name	<input type="text" value="itmsslmanual.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
* DNS	<input type="text" value="itmsslmanual.appviewx.com"/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	
* Hash Function	<input type="text" value="SHA256"/>	
* Key Type	<input type="text" value="RSA"/>	
* Bit Length	<input type="text" value="2048"/>	






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

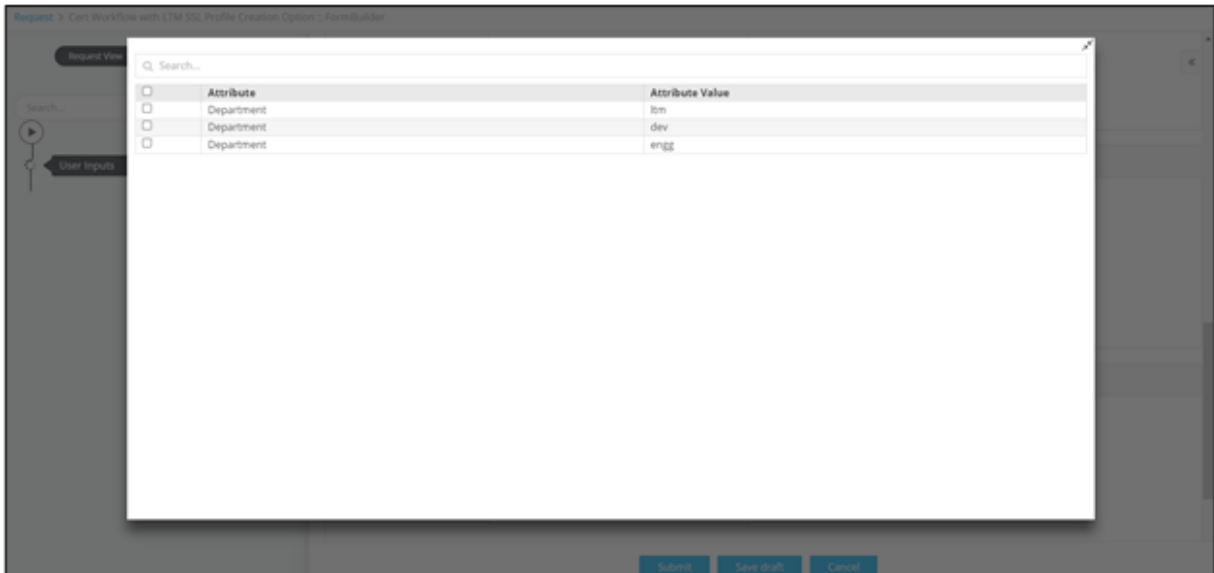
Field	Description
*Common Name	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.

Field	Description
Subject Alternative Name	Select the SAN as either: <ul style="list-style-type: none"> • DNS • IP Address
DNS	Enter a valid DNS if you select the DNS option in the SAN field. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field is displayed if DNS is selected in the The email id of the logged in user is populated automatically. field. </div>
IP Address	Enter a valid IP Address if you select the IP Address option in the SAN field. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field is displayed if IP Address is selected in the Subject Alternative Name field. </div>
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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>

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

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

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

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ LTM SSL Profile

* Device Vendor


* Device

* Profile Type

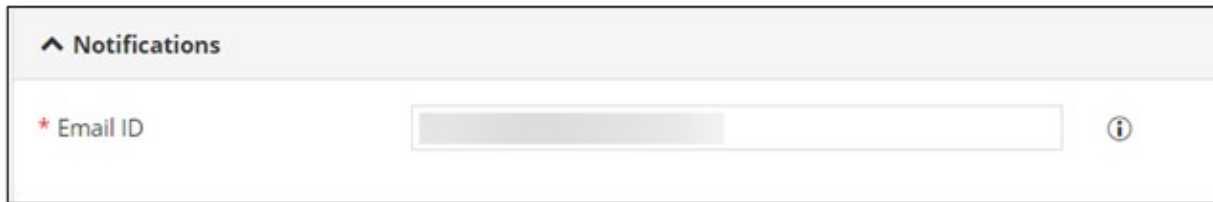
* Profile Name


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.	

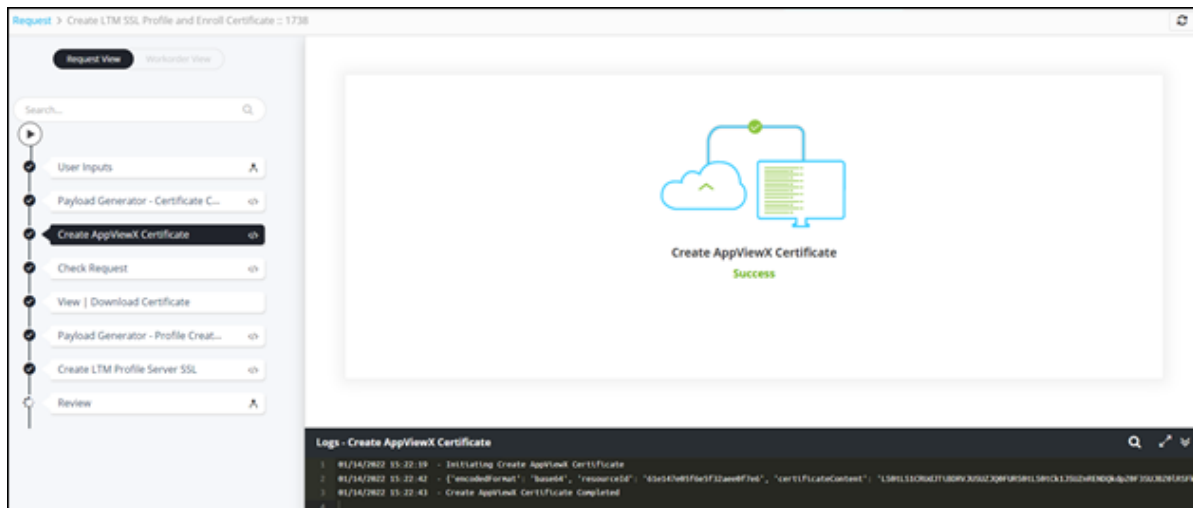
12. Under the **Email Notification** section, enter the email address(es).



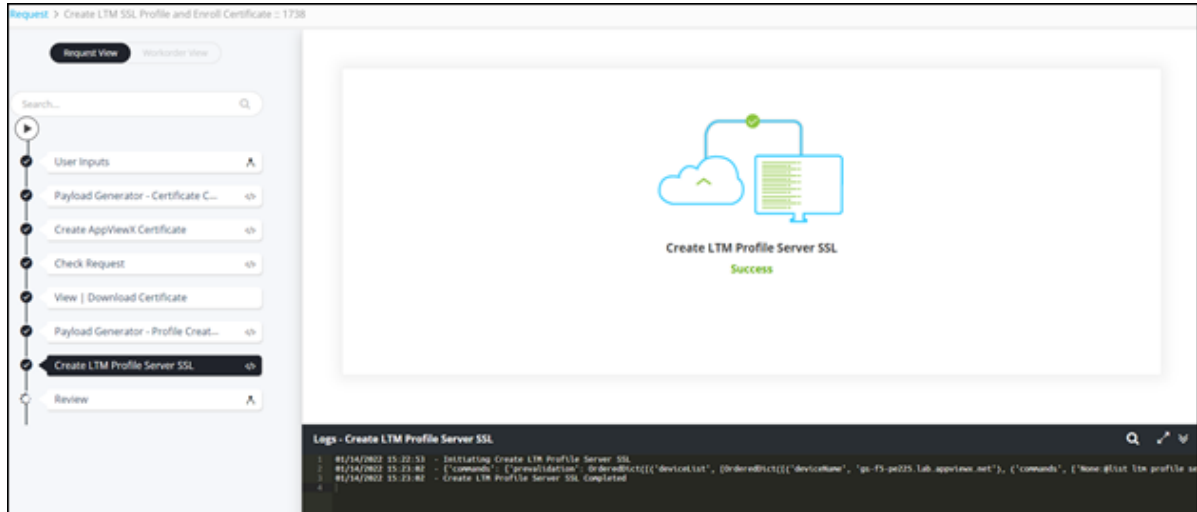
 **Note:** The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.

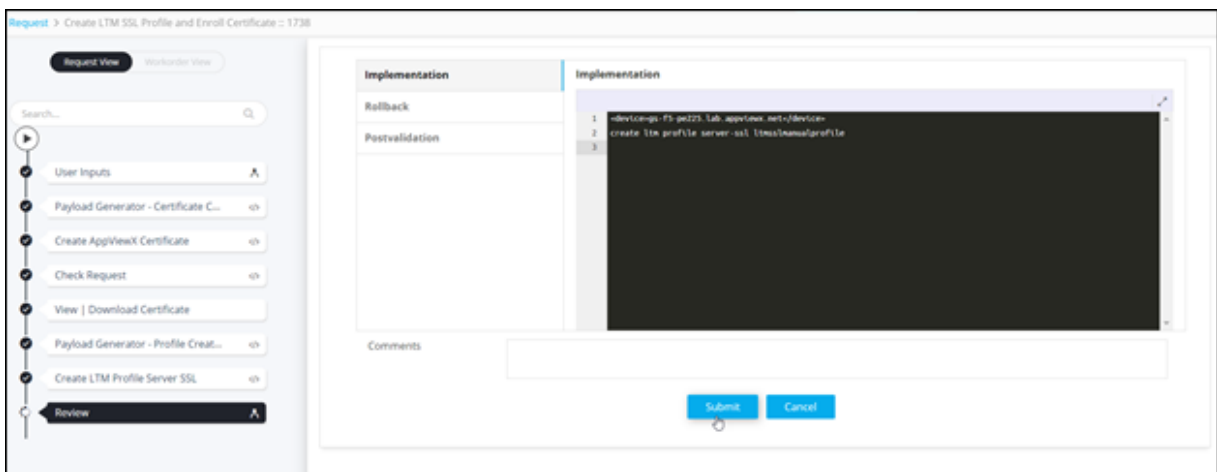
- AppViewX Certificate is generated successfully.



- LTM Profile on Server SSL created successfully.

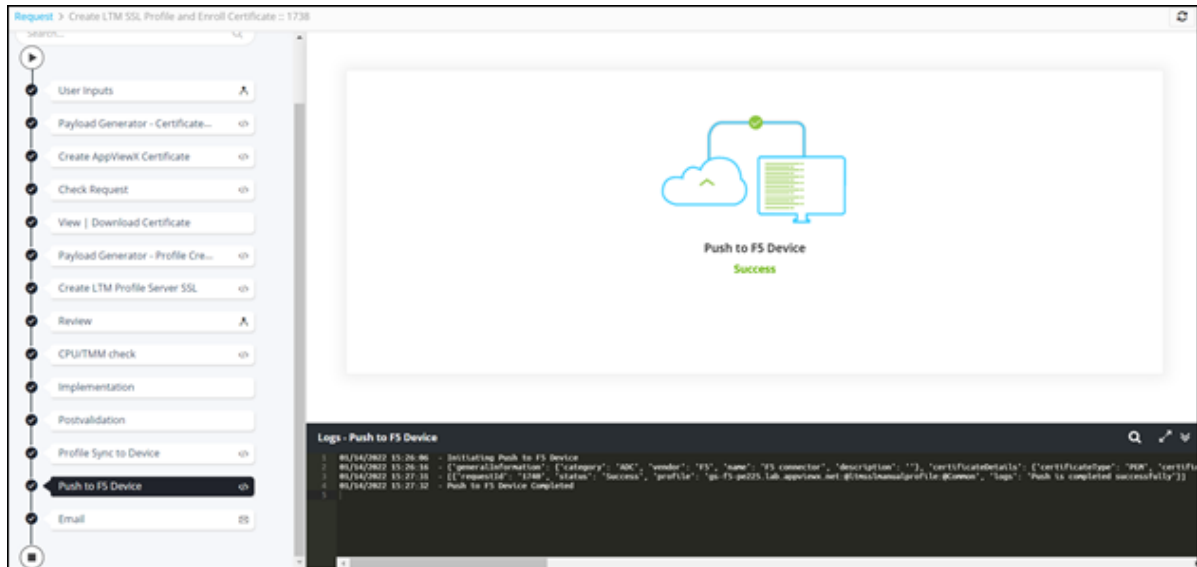


14. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

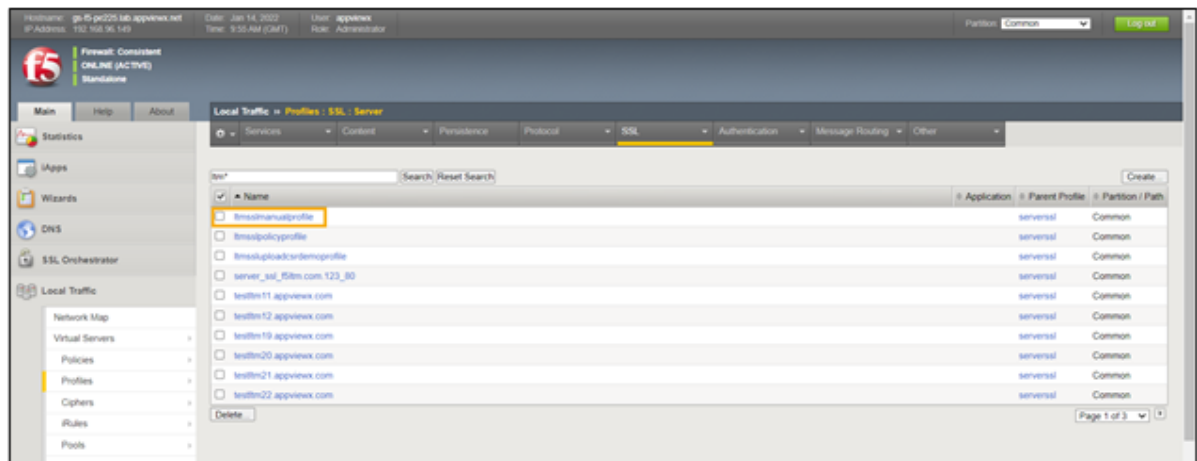


Note: You can change the profile name at this stage.

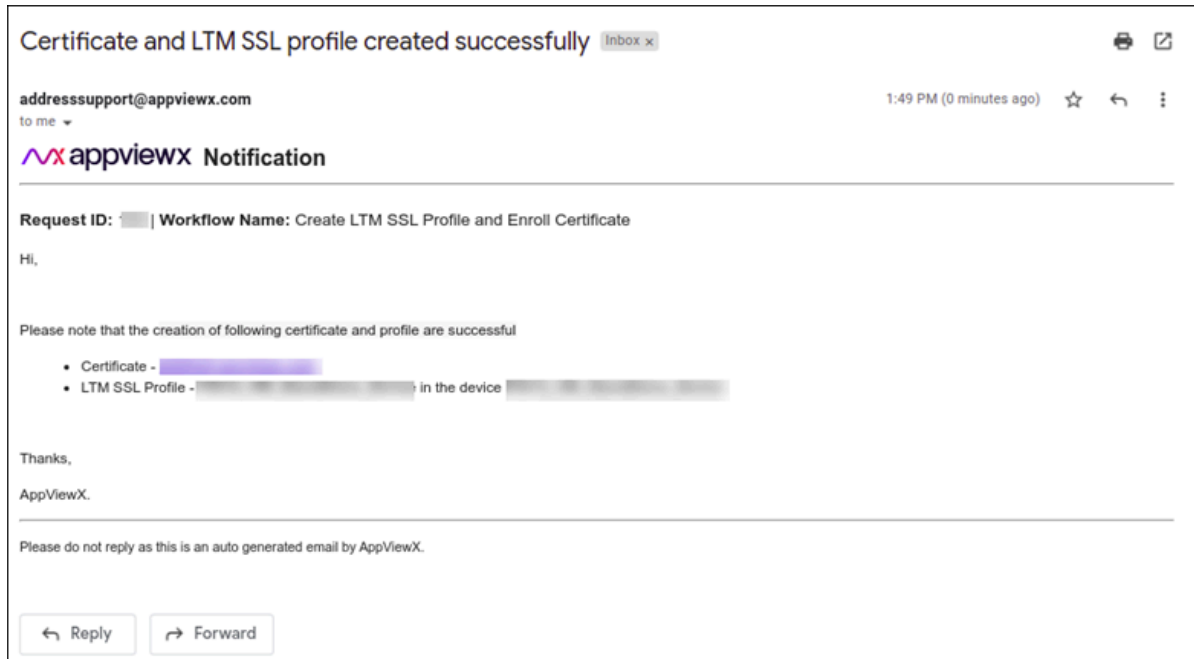
- Profile created on the selected F5 device.



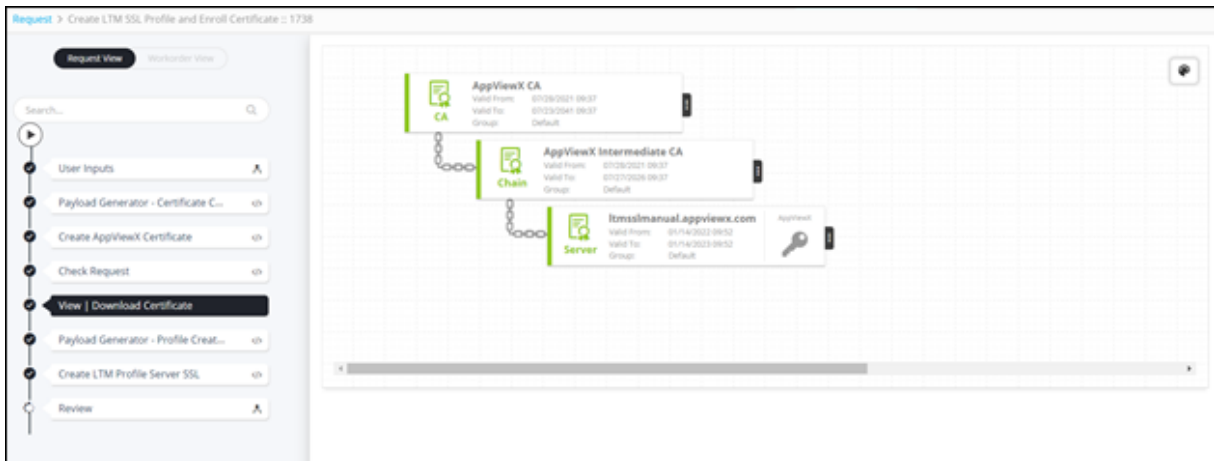
- Profile pushed to the selected F5 device.



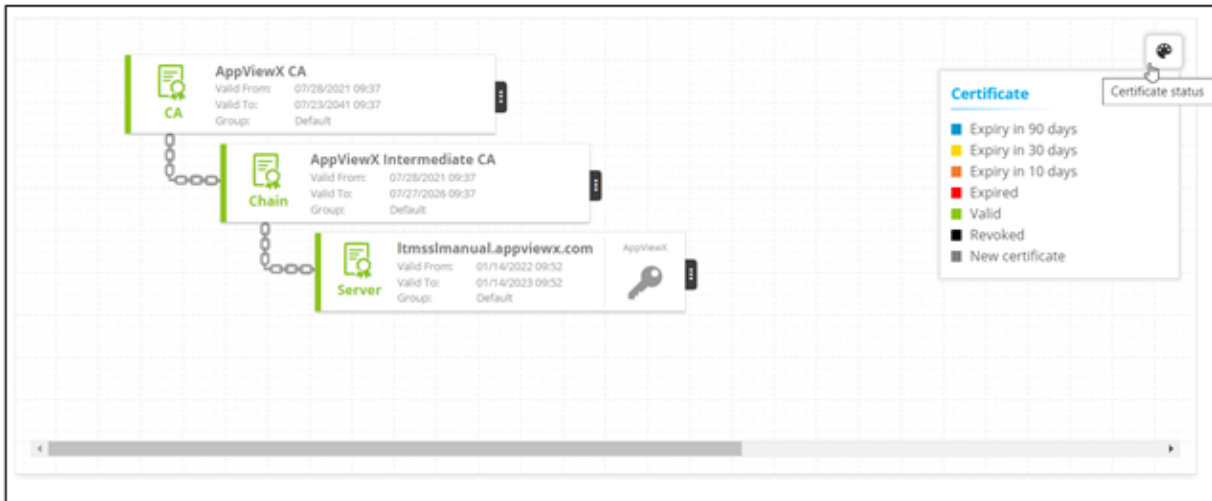
- Email notification received.



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**.






^ CSR Parameters

* Common Name	<input type="text" value="itmsslpolicy.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
* DNS	<input type="text" value="itmsslpolicy.appviewx.com"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text" value="Product Engineering"/>	
Locality	<input type="text" value="San Diego"/>	
State	<input type="text" value="Texas"/>	
Country	<input type="text" value="US"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	
* Hash Function	<input type="text" value="SHA256"/>	
* Key Type	<input type="text" value="RSA"/>	
* Bit Length	<input type="text" value="2048"/>	



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.

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ LTM SSL Profile


* Device Vendor

* Device

* Profile Type

* Profile Name

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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated on the basis of the selected device vendor. </div>
* 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).

^ Notifications

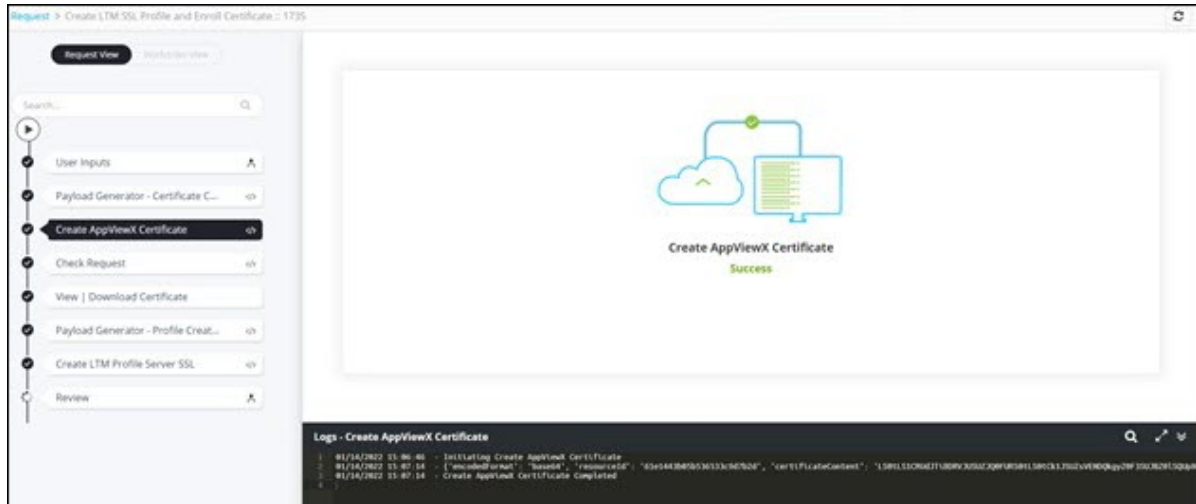
* Email ID



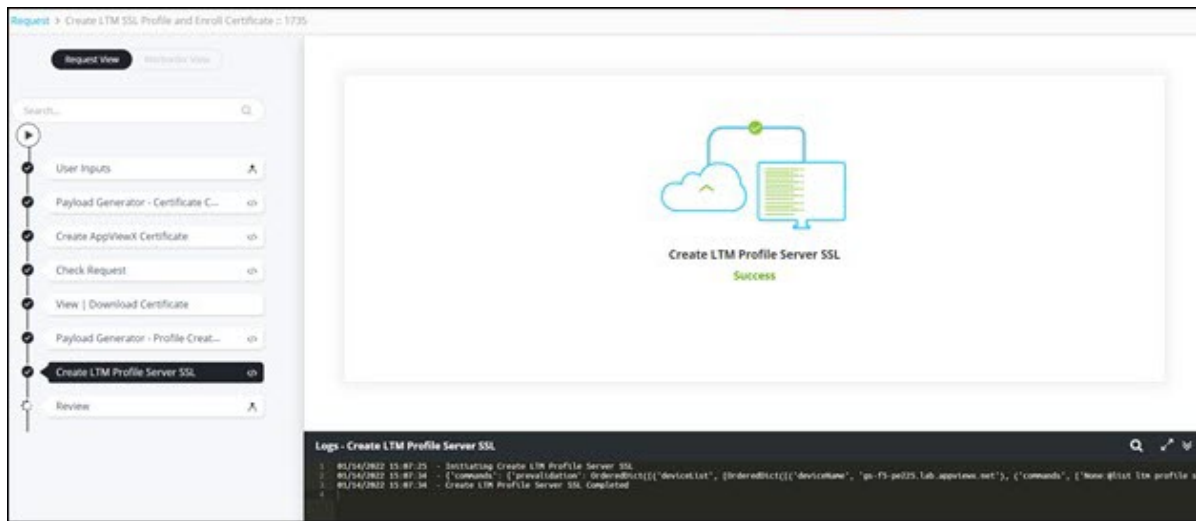
Note: The **User email** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address(es) in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.

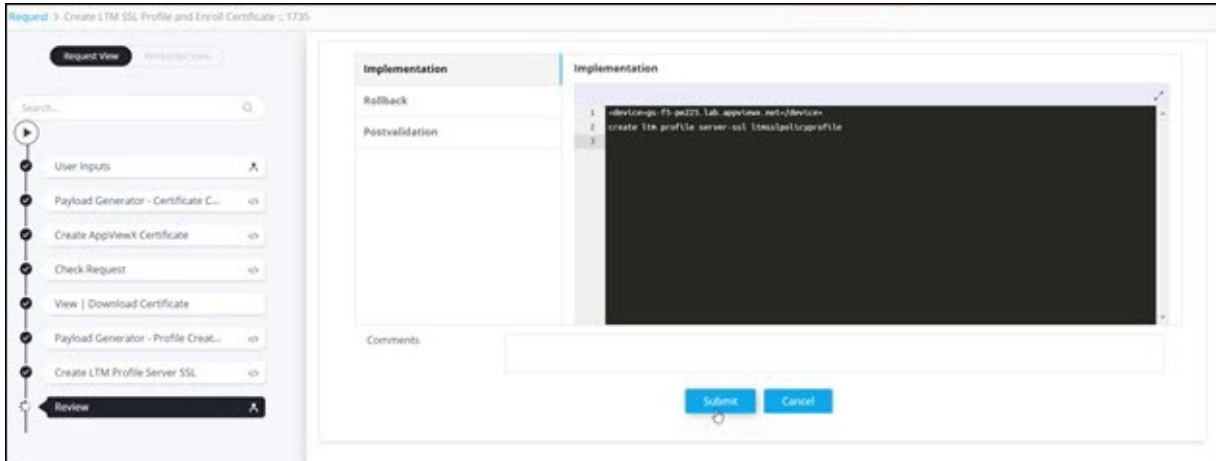
- AppViewX Certificate is generated successfully.



- LTM Profile on Server SSL created successfully.



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

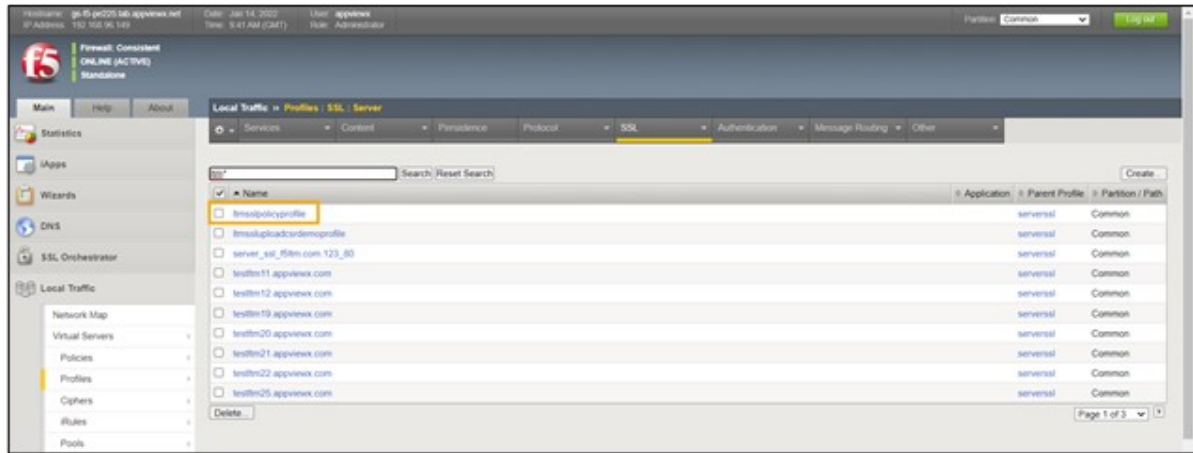


Note: You can change the profile name at this stage.

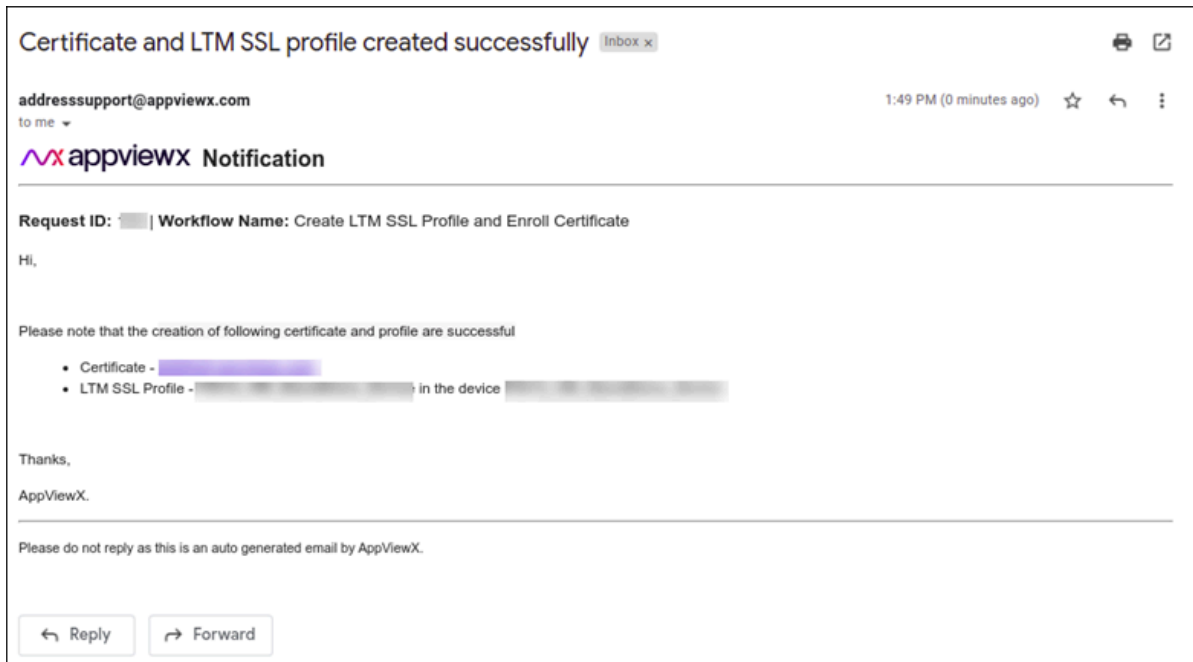
- Profile created on the selected F5 device.



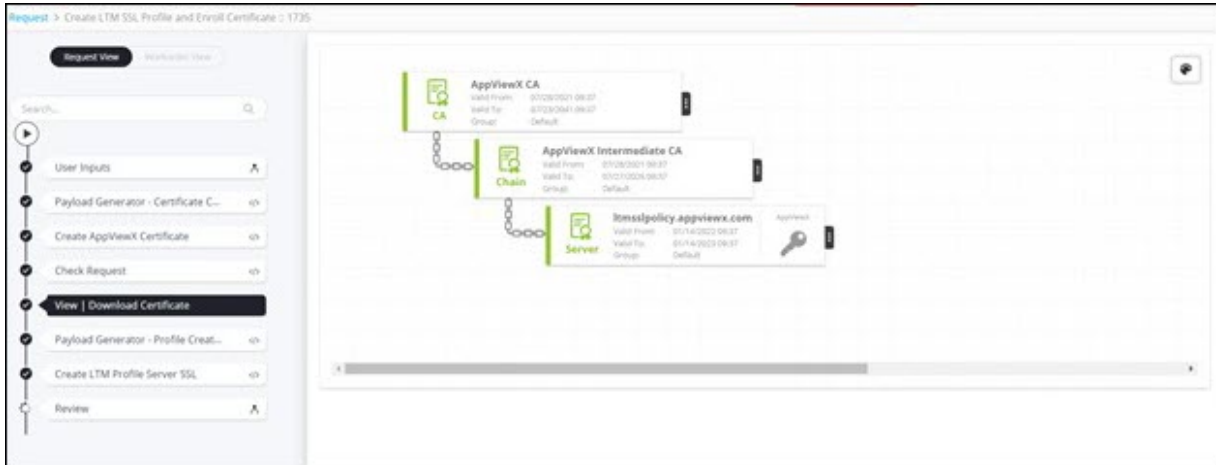
- Profile pushed to the selected F5 device.



- Email notification received.



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




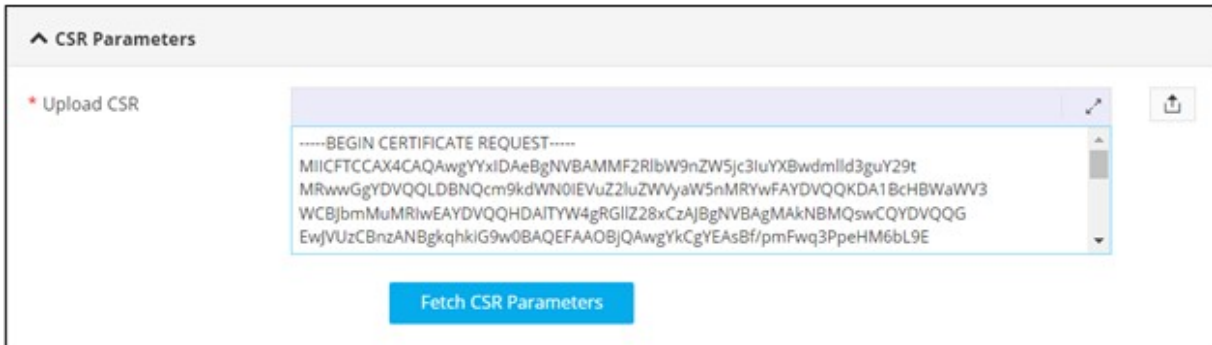
16. Hover your mouse over  to view the **Certificate status**.



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 .



CSR Parameters

* Upload CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIICFTCCAX4CAQAwgYYxiDAeBgNVBAMMF2RibW9nZW5jc3luYXBwdmllid3guY29t
MRwwGgYDVQQQLDBNQcm9kdWN0IEVuz2luZWVyaW5nMRYwFAYDVQQKDA1BcHBWYWV3
WCBJbmMuMRlwEAYDVQQQHDAlTYW4gRGlIZ28xCzAJBgNVBAGMAkNBMQswCQYDVQQG
EwjVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA5Bf/pmFwq3PpeHM6bL9E
```

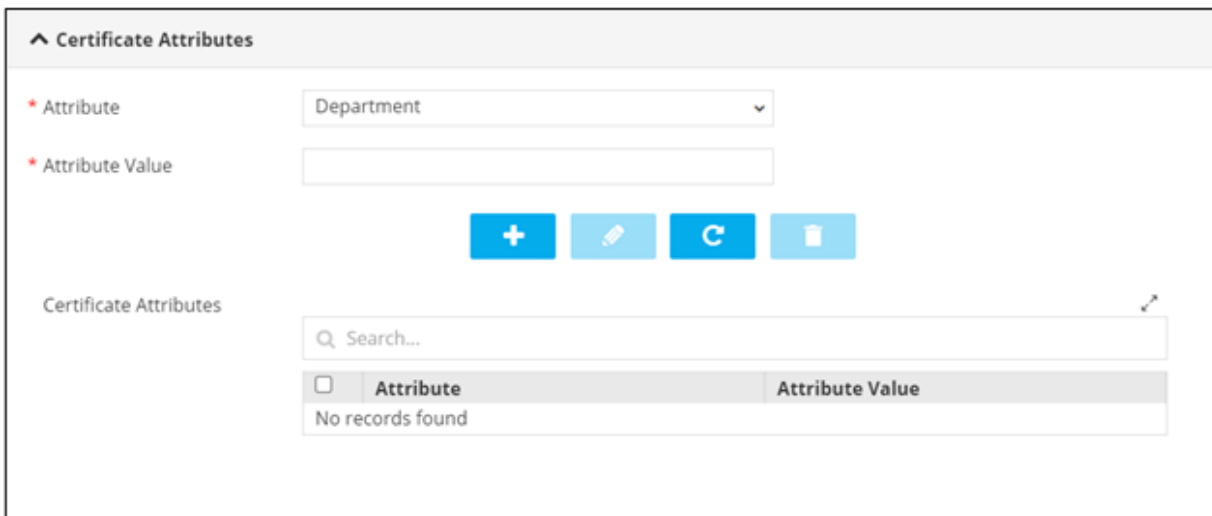
Fetch CSR Parameters

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.



Certificate Attributes

* Attribute: Department






* Attribute Value:

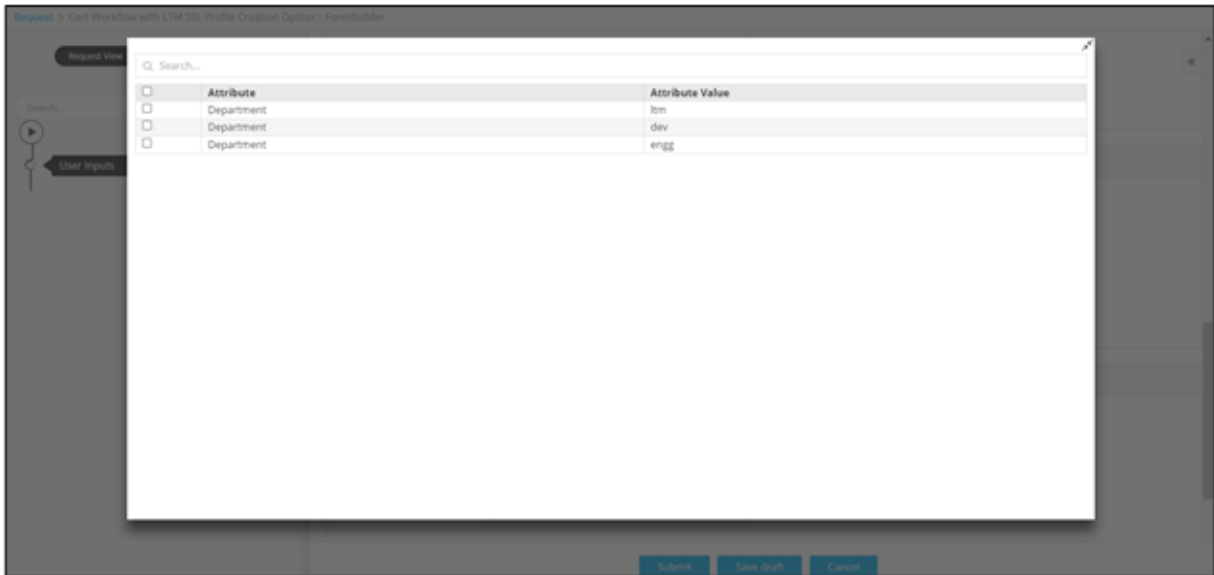
+ ✎ ↻ 🗑️

Certificate Attributes

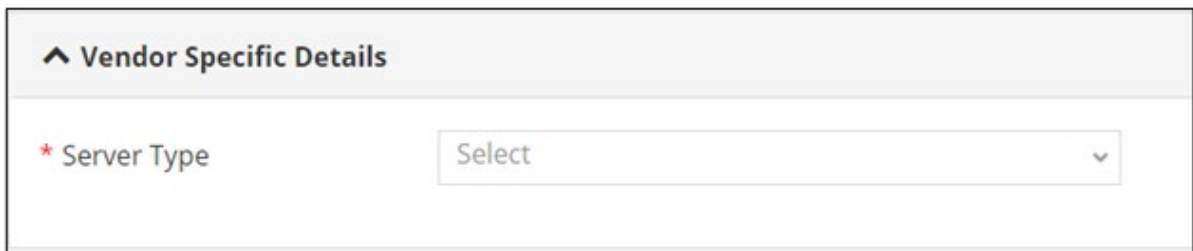
Search...

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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.

^ LTM SSL Profile

* Device Vendor


* Device

* Profile Type

* Profile Name

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).

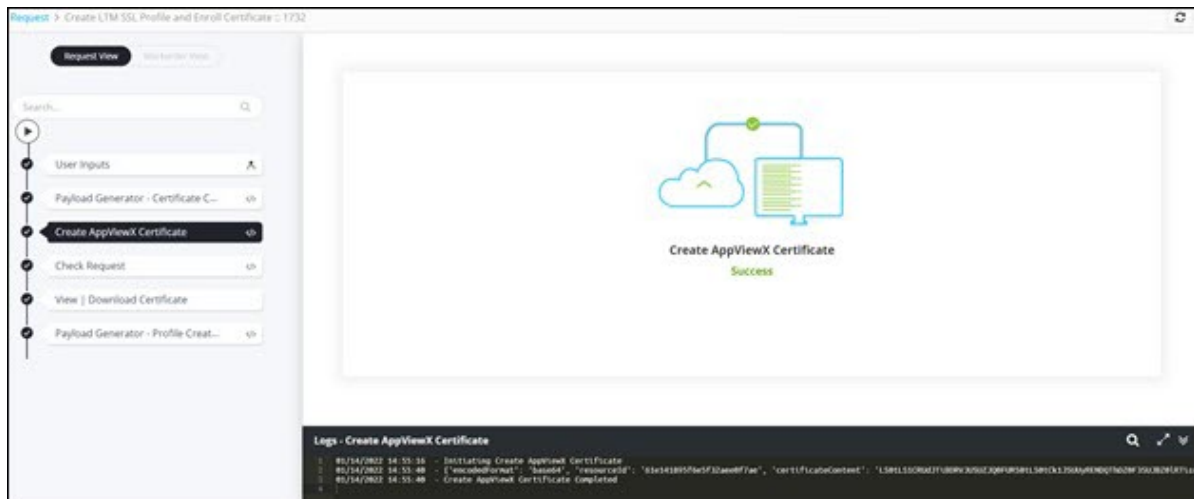
Notifications

* Email ID

 **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**.

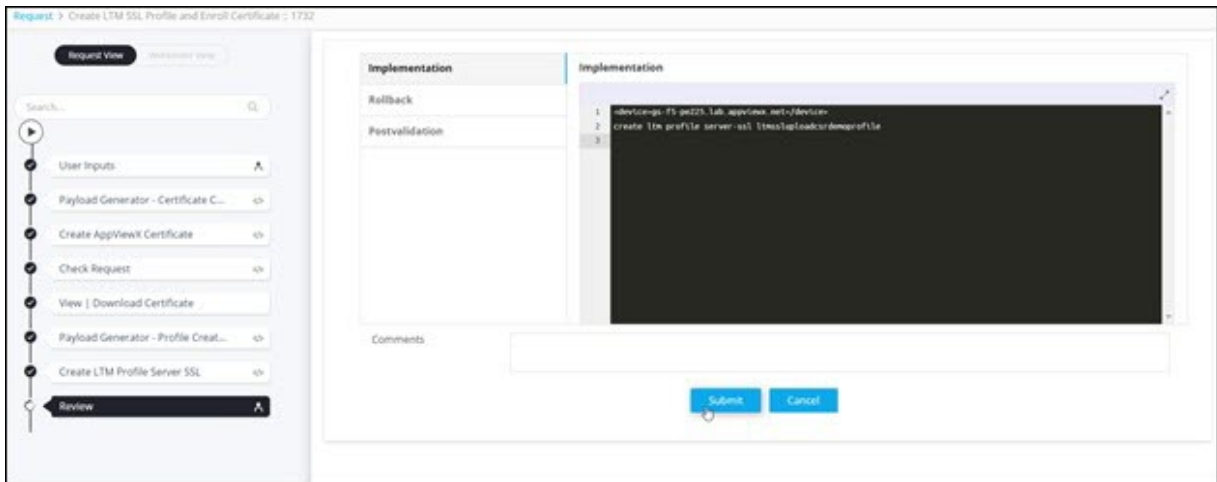
- AppViewX Certificate generated.



- LTM Profile on Server SSL created successfully.

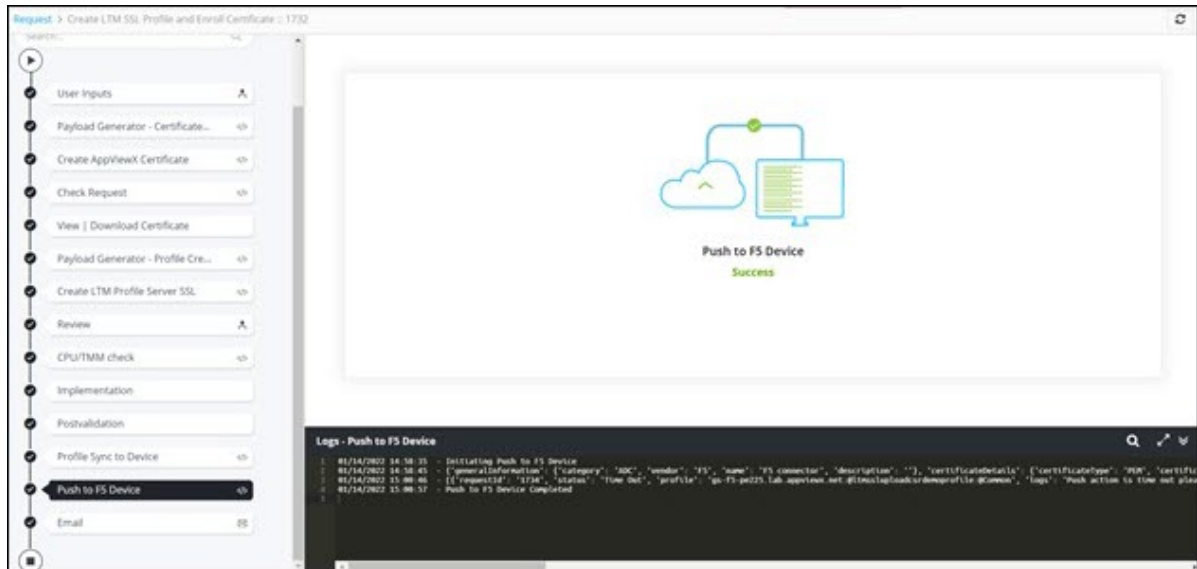


15. At the **Review** stage of workflow execution, review the device and profile name and click **Submit**.

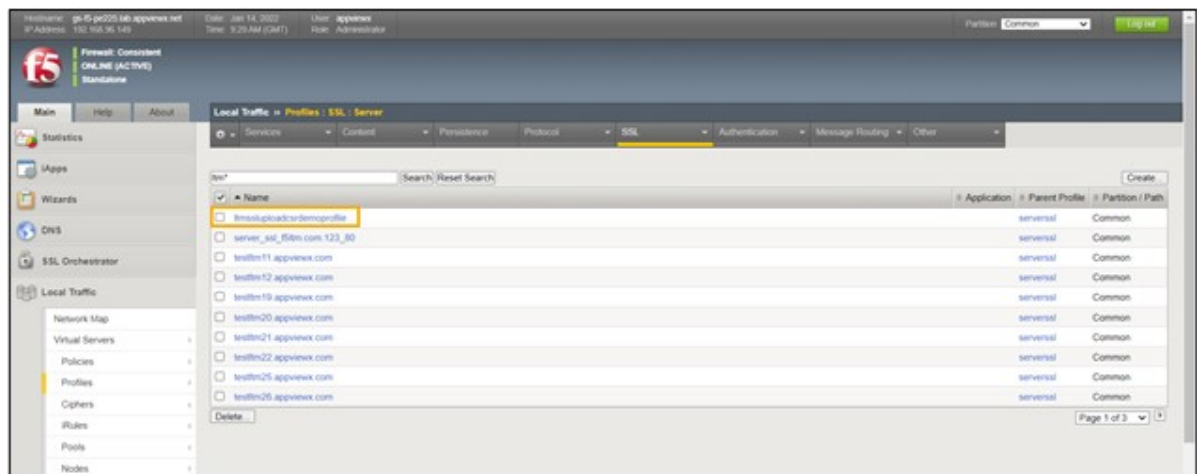


Note: You can change the profile name at this stage.

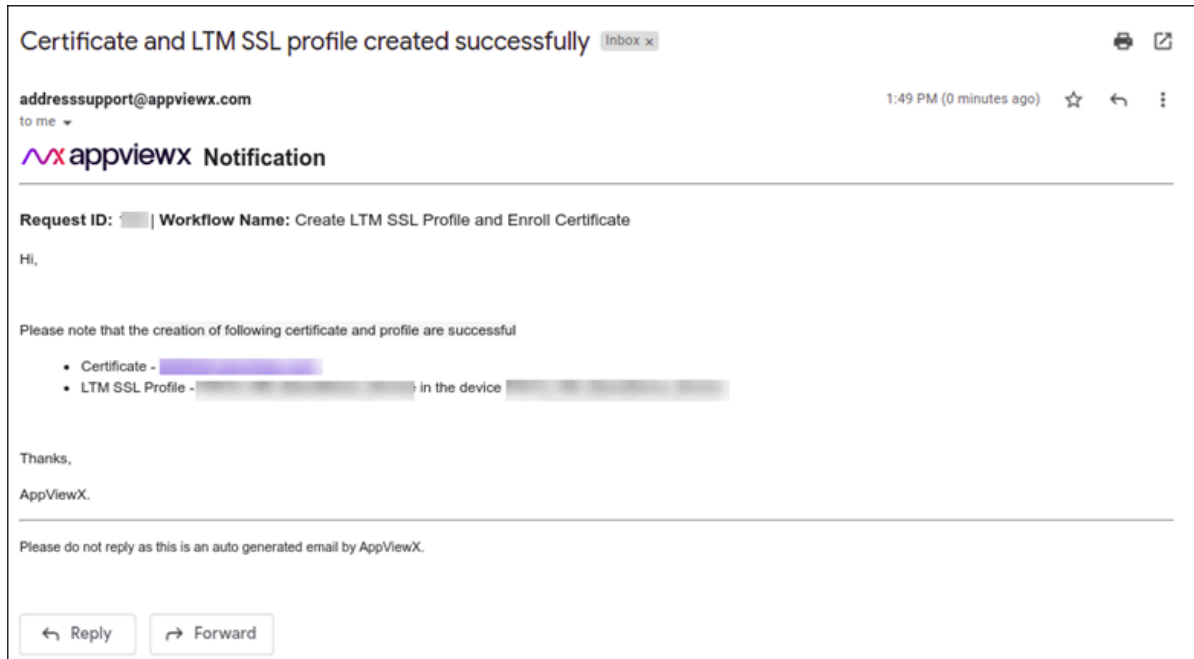
- Profile created on the selected F5 device.



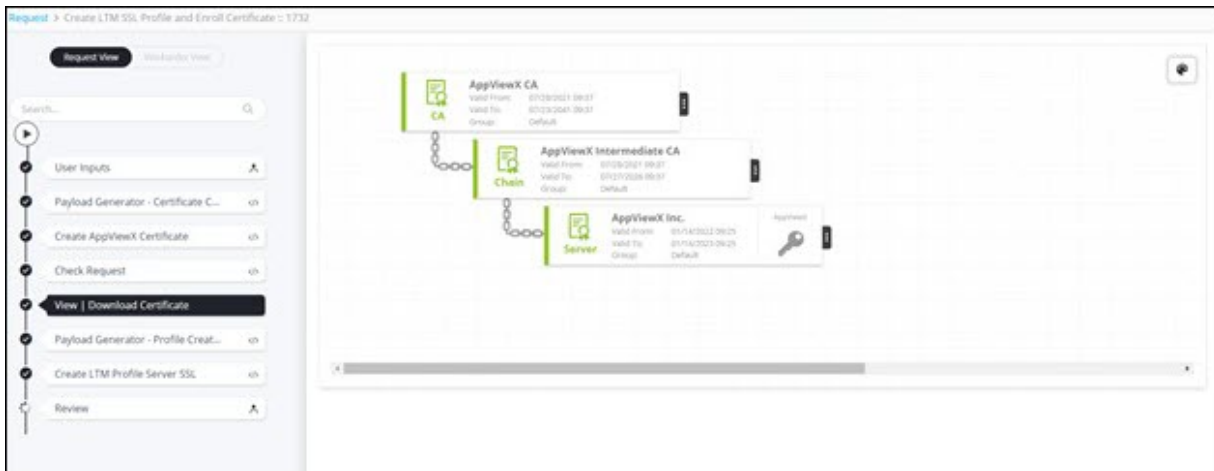
- Profile pushed to the selected F5 device.



- 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**.



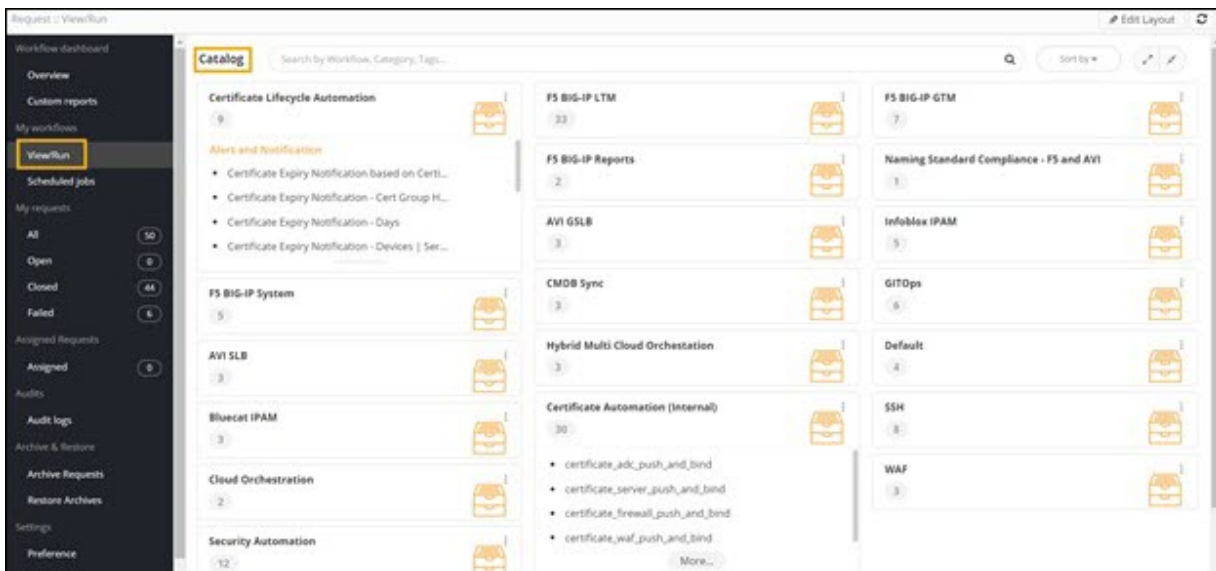
Enroll Certificate with Certificate Group and CSR Upload



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.

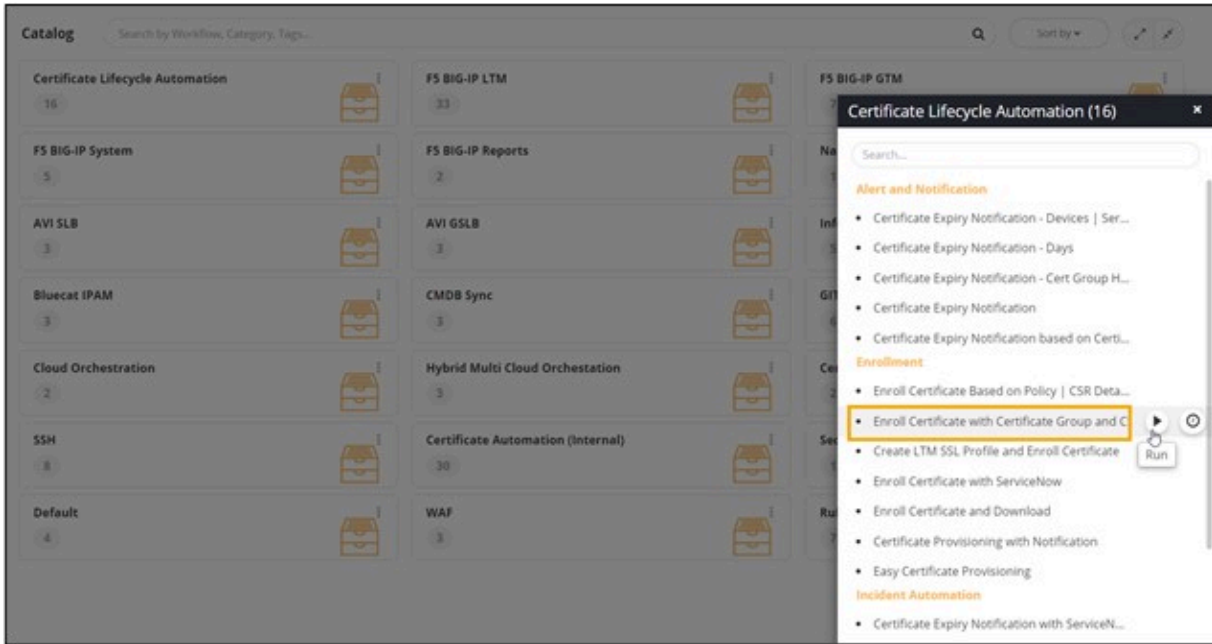
To trigger this workflow:


1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.

The workflow **Catalog** page is displayed.

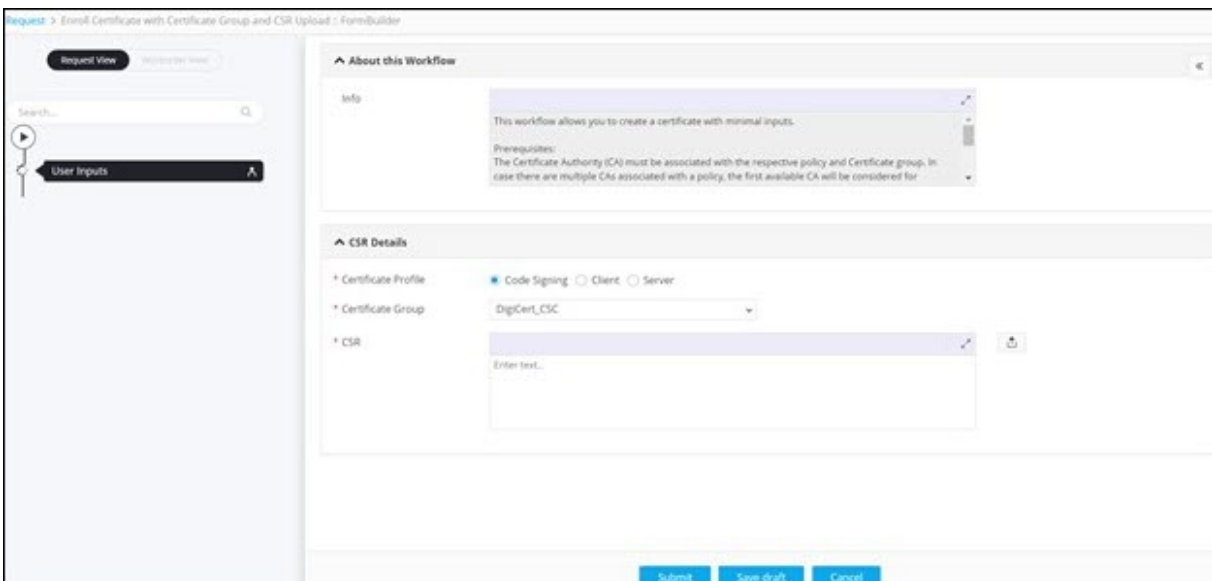


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate with Certificate Group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


CSR Details

* Certificate Profile Code Signing Client Server

* Certificate Group

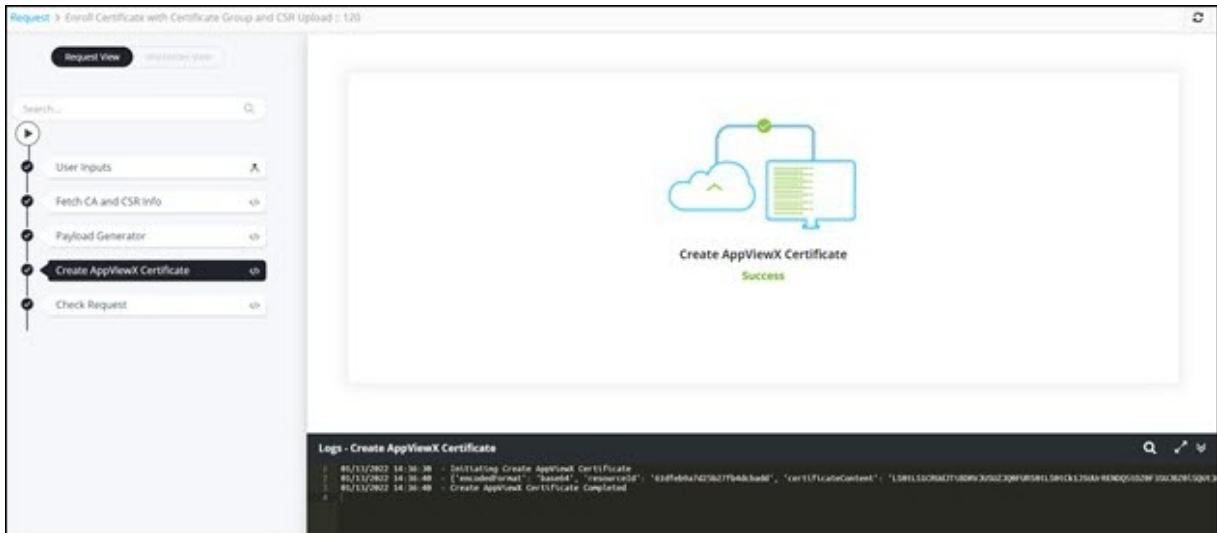
* CSR


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

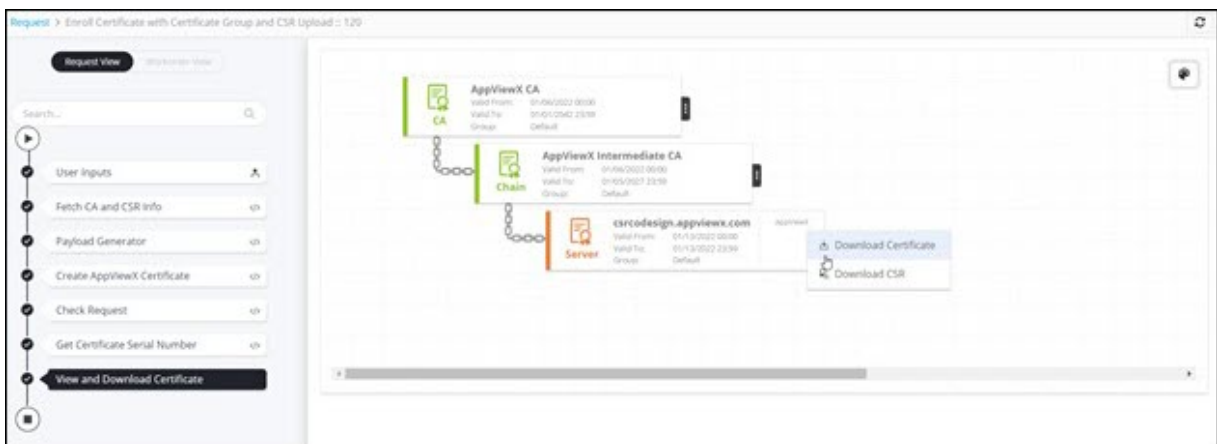
Field	Description
* Certificate Profile	Select the Certificate Profile from the following options: <ul style="list-style-type: none"> • Code Signing • Server • Client Note: Server is the default selection.
* Certificate Group	Select the Certificate Group from the options available in the dropdown.
* 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.



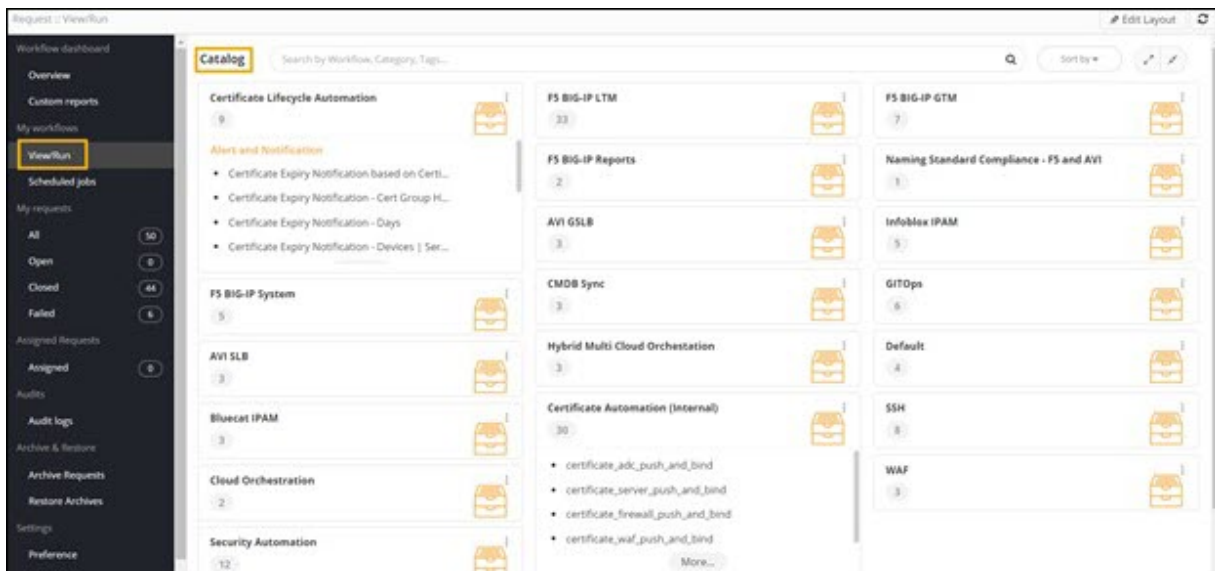
Enroll Certificate With ServiceNow

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


To trigger this workflow:

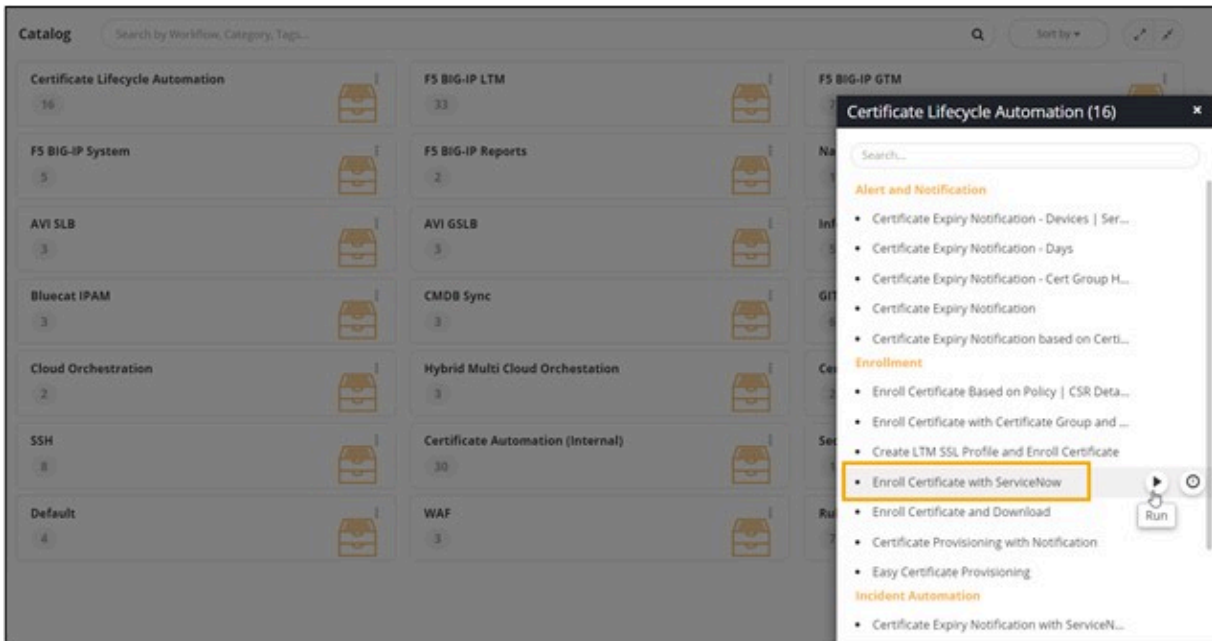
1. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.


The workflow **Catalog** page is displayed.



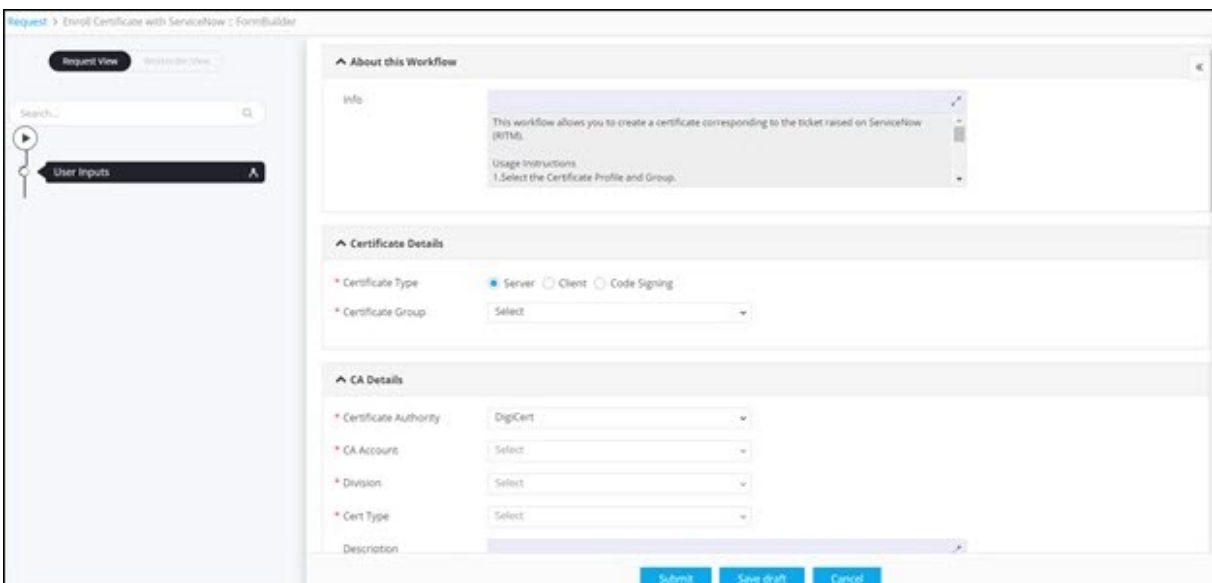
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.

- 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.



- 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
*CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the CA selected. </div>
*Division	Select the Division from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when DigiCert is selected as the CA. </div>
*Cert Type	Select the Cert Type from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when DigiCert or Entrust are selected as the CA. </div>
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:

^ CSR Parameters		
* Common Name	<input type="text" value="certwithsnow.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certwithsnow.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text" value="Product Engineering"/>	
Locality	<input type="text"/>	
State	<input type="text" value="Texas"/>	
Country	<input type="text" value="US"/>	
Email Address	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
* Key Type	RSA
* Bit Length	2048
* Hash Function	SHA256
* Download Format	PEM (*.crt)

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

^ Certificate Attributes






* Attribute

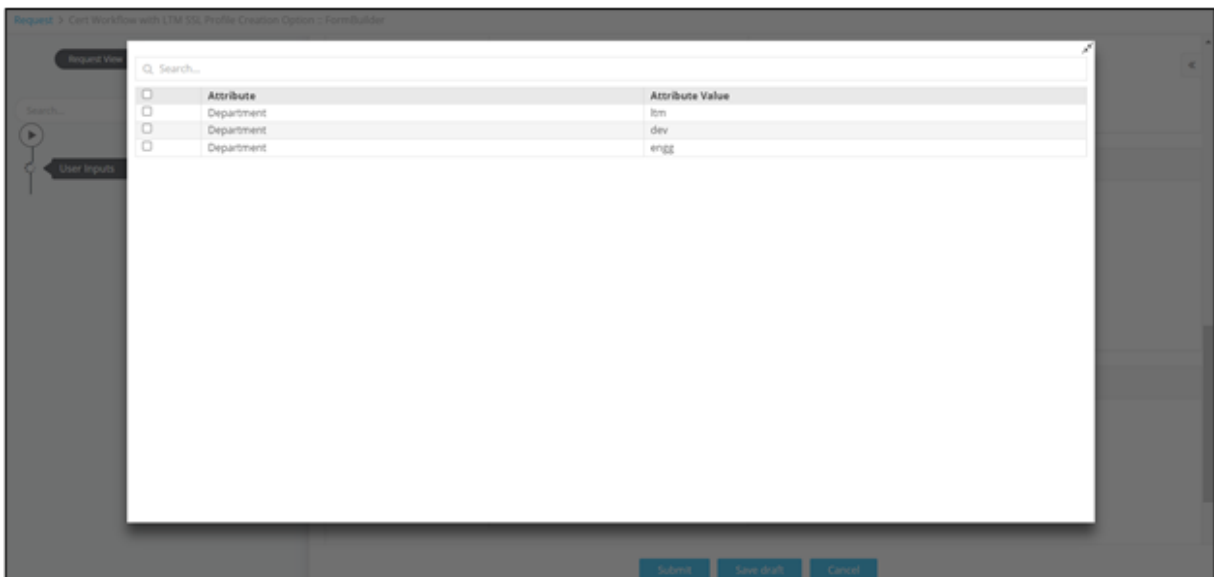
* Attribute Value

+
✎
C
✖

Certificate Attributes

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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.

Vendor Specific Details

* Server Type Select 

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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).

^ ServiceNow Details

* RITM Ticket Number

* ServiceNow Account

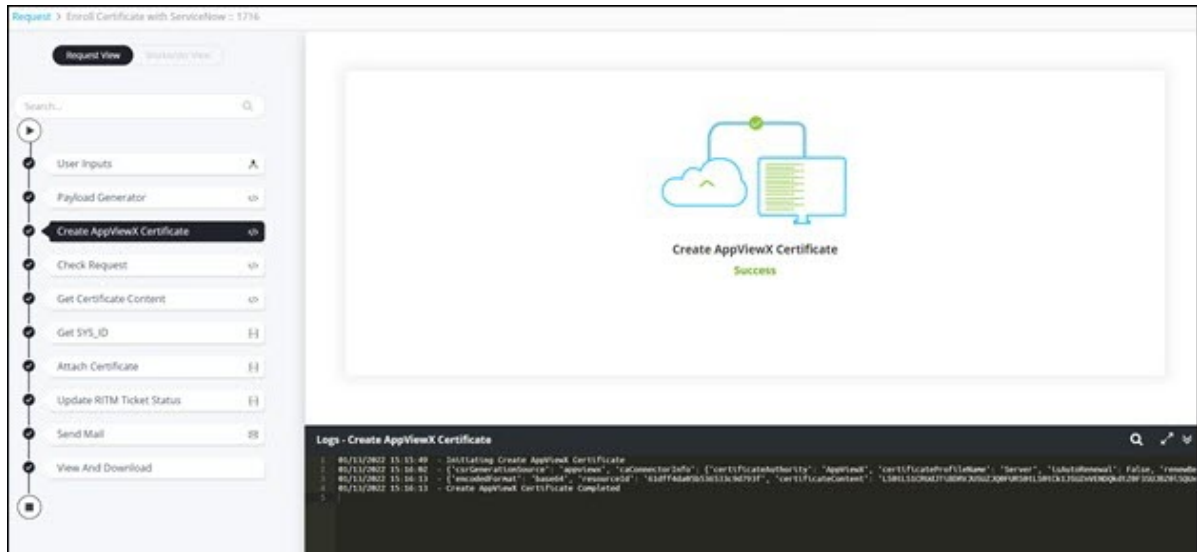
19. Under the **Notifications** section, enter the email address to which the certificate details have to be sent.

^ Notifications

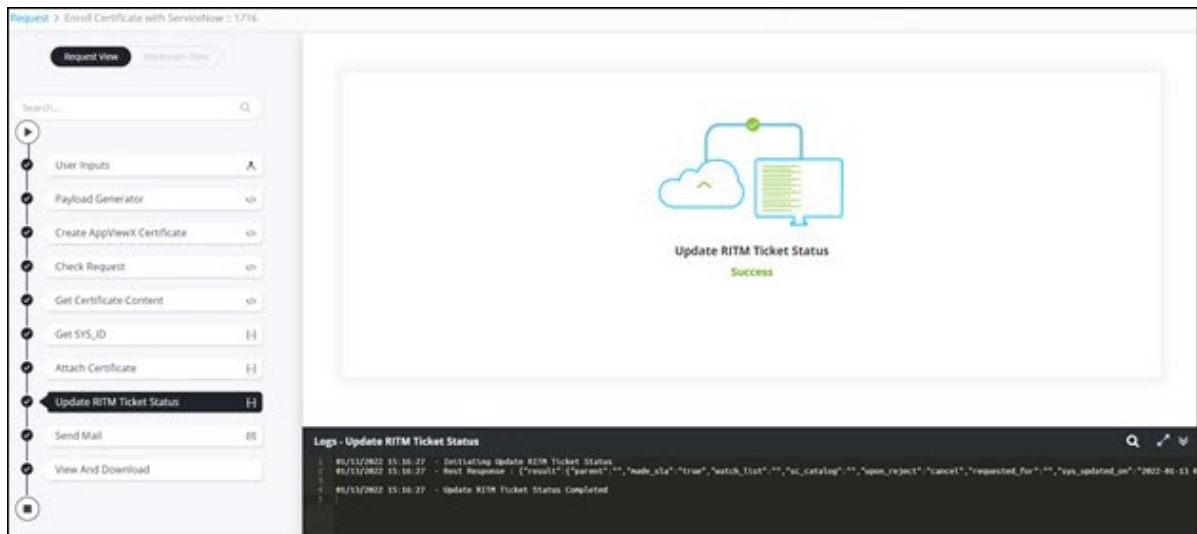
* Email ID 

20. Click **Submit**.

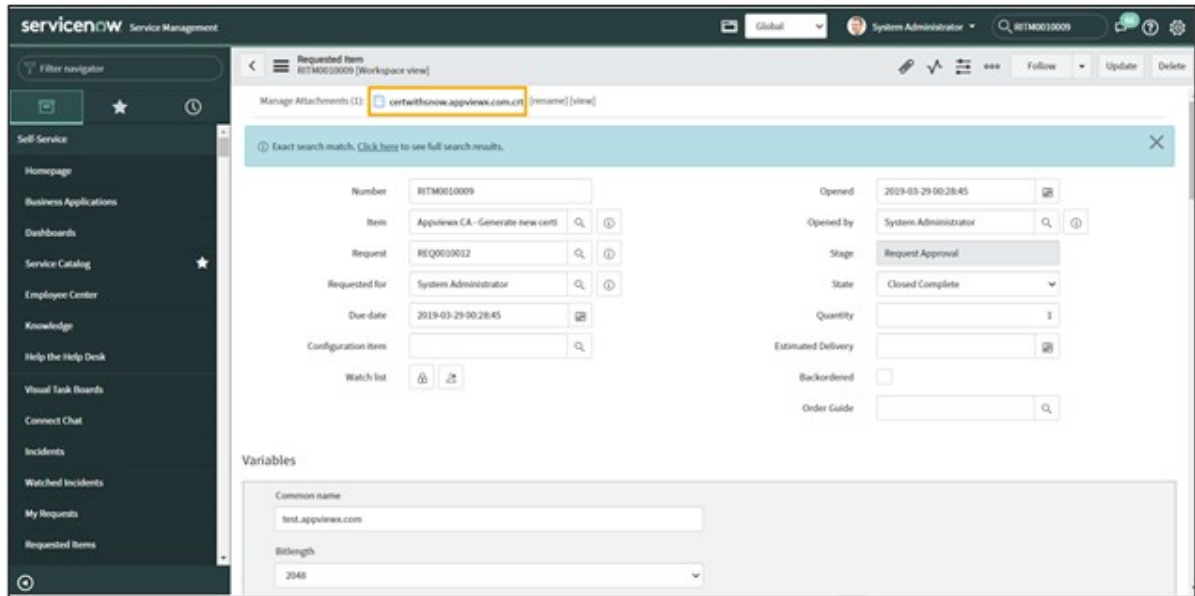
- AppViewX Certificate is created successfully.



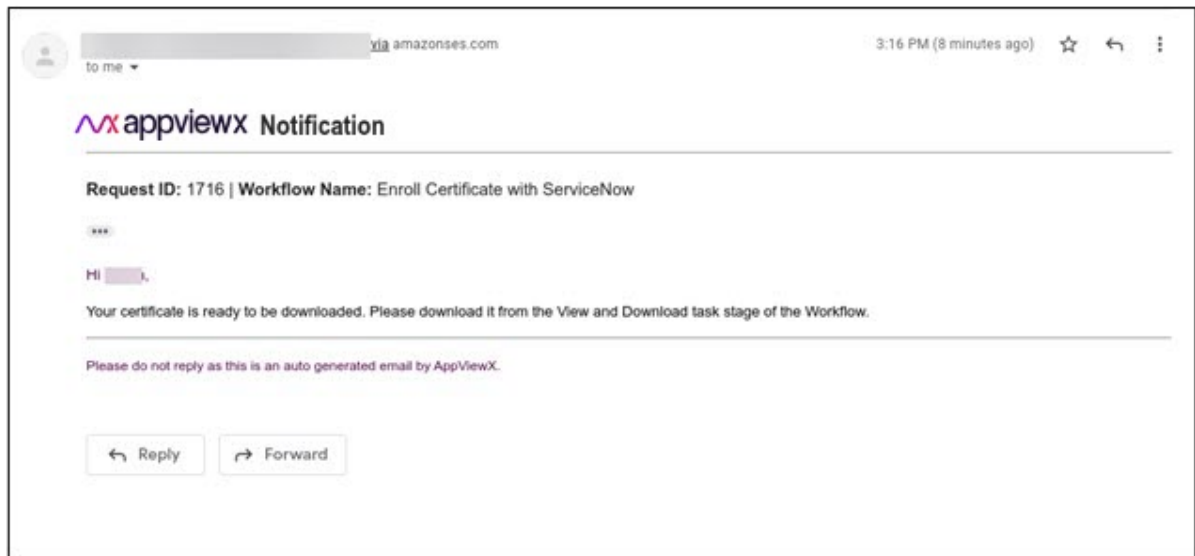
- RITM ticket status updated.



- Certificate updated in the ServiceNow ticket.



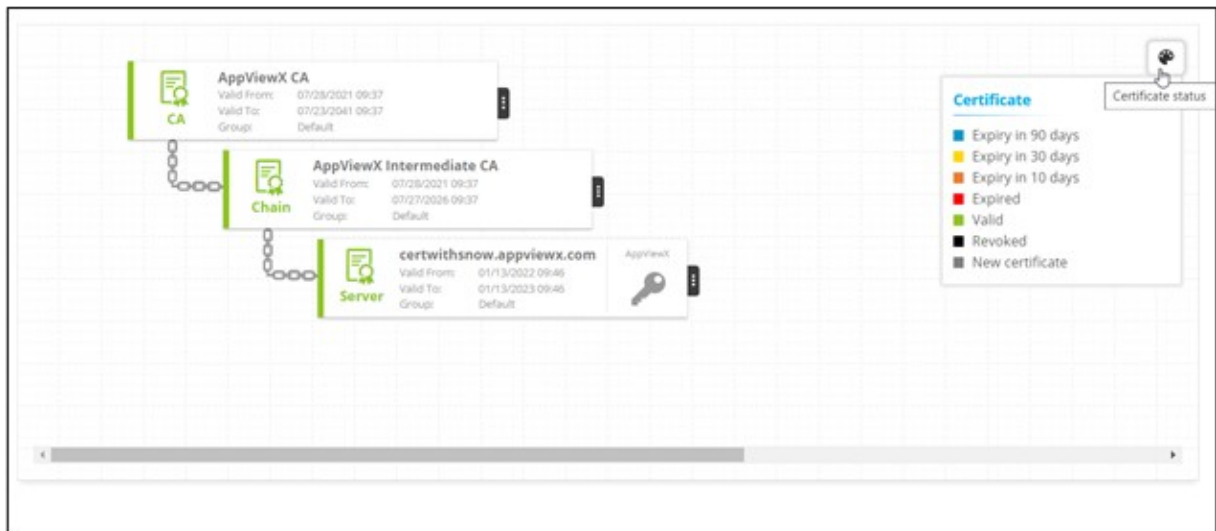
- Email notification received.



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.

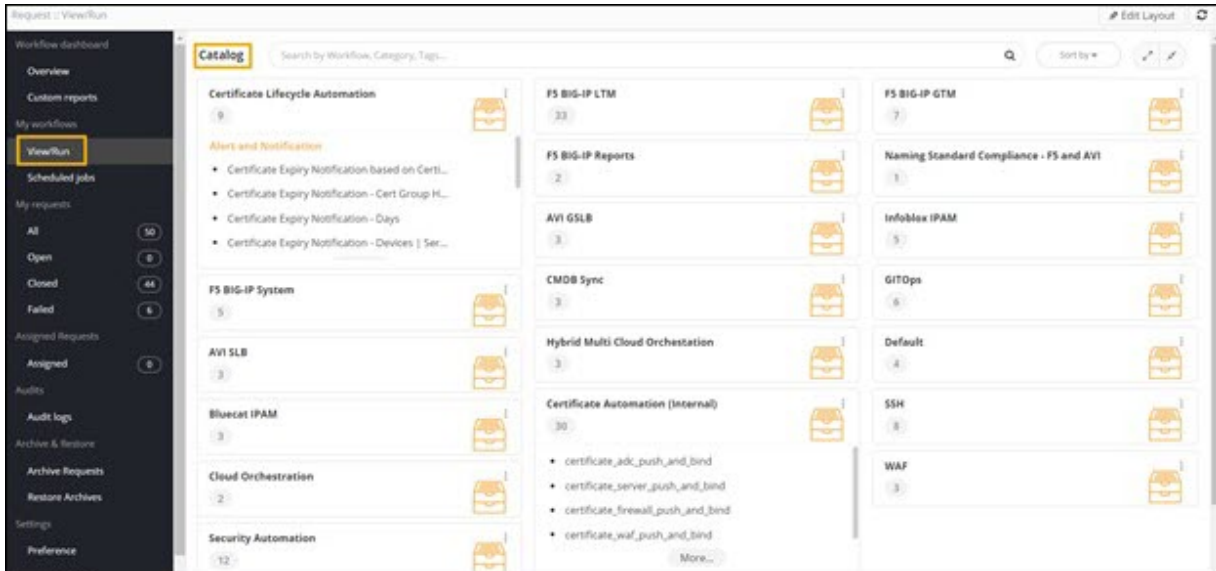




Enroll Certificate and Push with ServiceNow

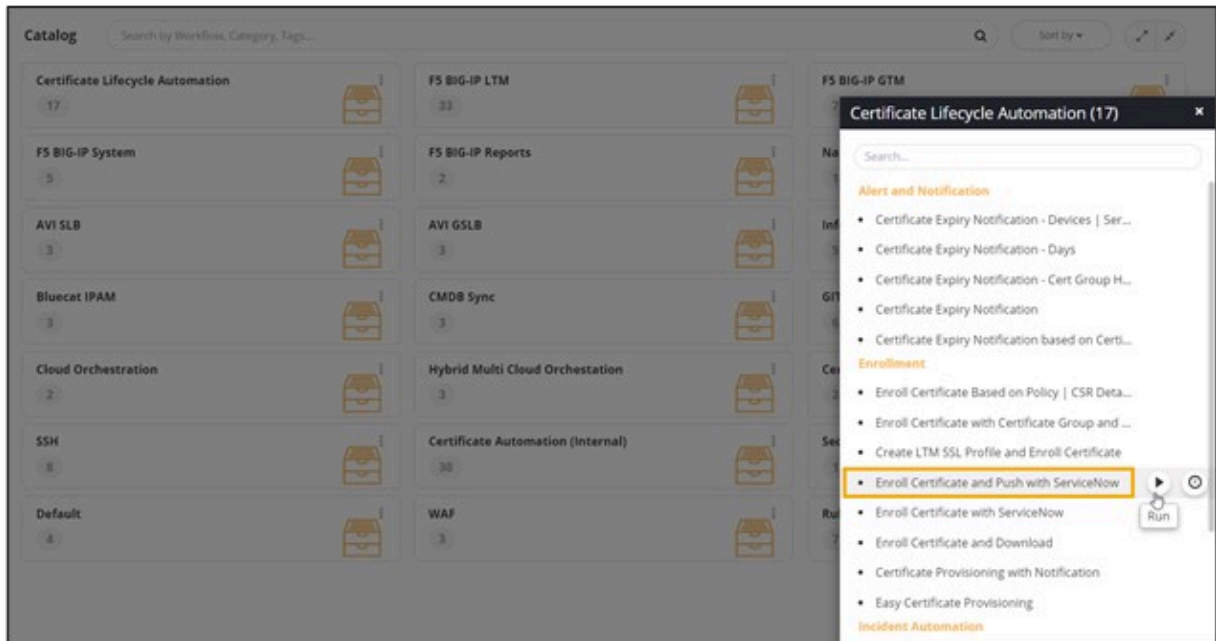
This workflow allows you to create a certificate corresponding to the ticket raised on ServiceNow (RITM) and push it to the selected device.

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.

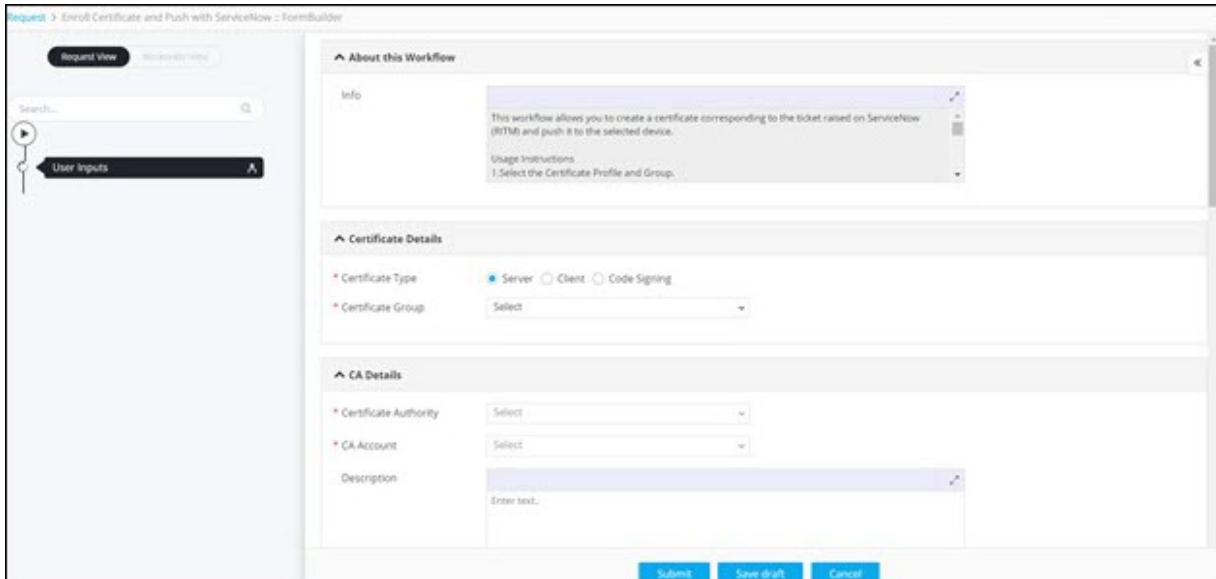


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click  .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Enrollment** category, hover your mouse over the **Enroll Certificate and Push with ServiceNow**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

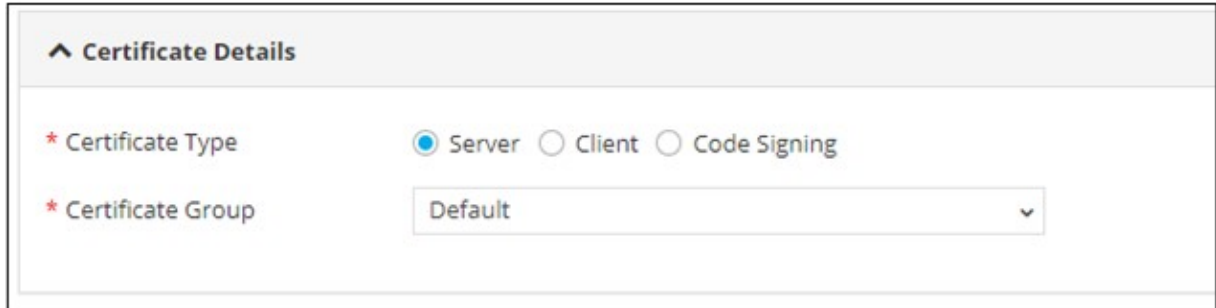


i **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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: <ul style="list-style-type: none"> • 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 screenshot shows a form titled "CA Details" with the following fields:

- * Certificate Authority**: A dropdown menu with "DigiCert" selected.
- * CA Account**: A dropdown menu with "Select" selected.
- * Division**: A dropdown menu with "Select" selected.
- * Cert Type**: A dropdown menu with "Select" selected.
- Description**: A text area with the placeholder text "Enter text..." and a small icon in the top right corner.







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

Field	Description
* Certificate Authority	Select the Certificate Authority from the available options: <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX
* CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the CA selected. </div>
* 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:


^ CSR Parameters

* Common Name	<input type="text" value="certcreateandpushsnow.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certcreateandpushsnow.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text" value="Product Engineering"/>	
Locality	<input type="text"/>	
State	<input type="text" value="Texas"/>	
Country	<input type="text" value="US"/>	
Email Address	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
* Key Type	Select
* Bit Length	Select
* Hash Function	Select
* Download Format	PEM (*.crt)

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

^ Certificate Attributes






* Attribute

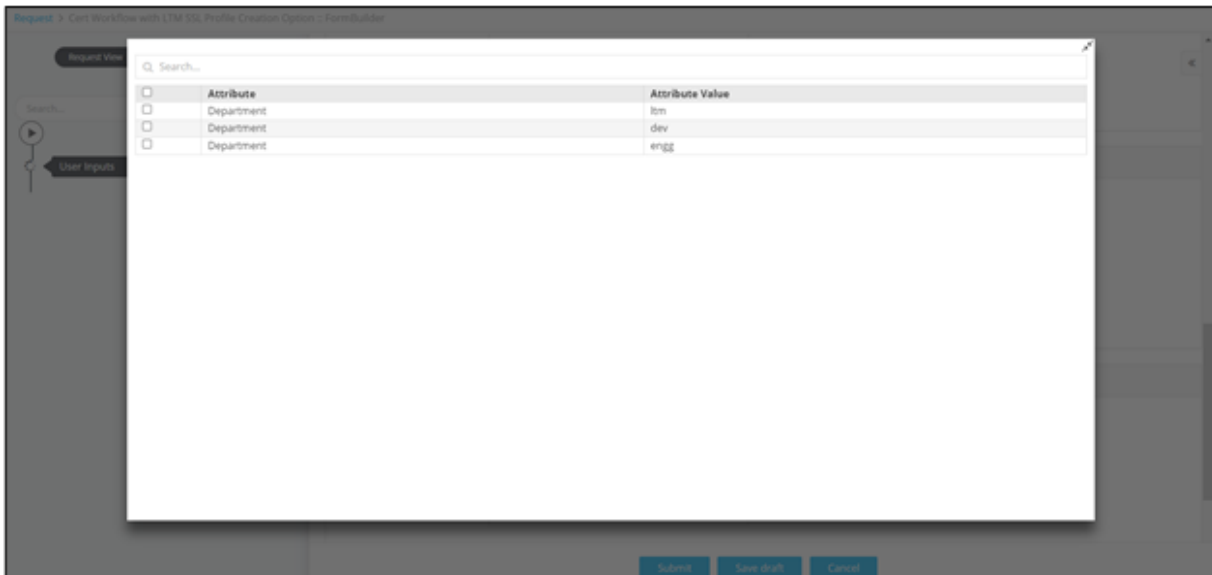
* Attribute Value

+
✎
C
✖

Certificate Attributes ↕

	Attribute	Attribute Value
No records found		




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.

Vendor	Device	Linux Actio...	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.l...	gs-f5-pe225.lab.appviewx.ne...	*****

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.

Device Details

* Device Type: ADC

* Vendor: F5

* Device: gs-f5-pe225.lab.appviewx.net

* Profiles/Application: gs-f5-pe225.lab.appviewx.net:@V13_Client_ssl:@Common

+ Edit Refresh Delete

Update

* Push to Devices

Search...

<input type="checkbox"/>	Vendor	Device	Linux Actions	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.lab...		gs-f5-pe225.lab.appvi...	*****
<input checked="" type="checkbox"/>	F5	gs-f5-pe225.lab...		gs-f5-pe225.lab.appvi...	*****



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.

* Push to Devices

Search...

<input type="checkbox"/>	Vendor	Device	Linux Actions	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.lab...		gs-f5-pe225.lab.appvi...	*****
<input type="checkbox"/>	F5	gs-f5-pe225.lab...		gs-f5-pe225.lab.appvi...	*****

gs-f5-pe225.lab.appviewx.net,gs-f5-pe225.lab.appviewx.net:@KAN:@rrr,gs-f5-pe225.lab.appviewx.net:@NYC_test_vip_dont_delete_client_ssl:@Common

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.

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name



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).

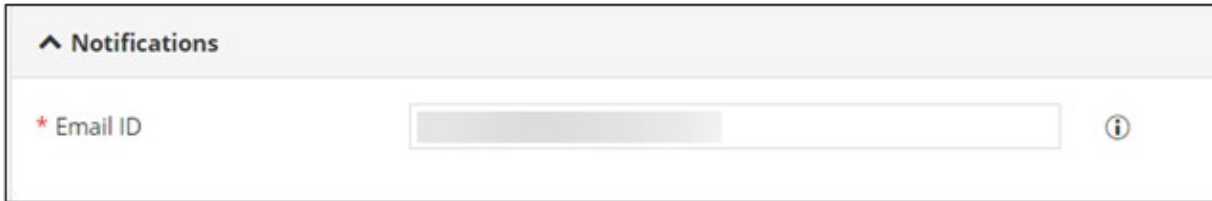
25. Under the **ServiceNow Details** section, select the **ServiceNow Account** (mandatory).

^ ServiceNow Details

* RITM Ticket Number

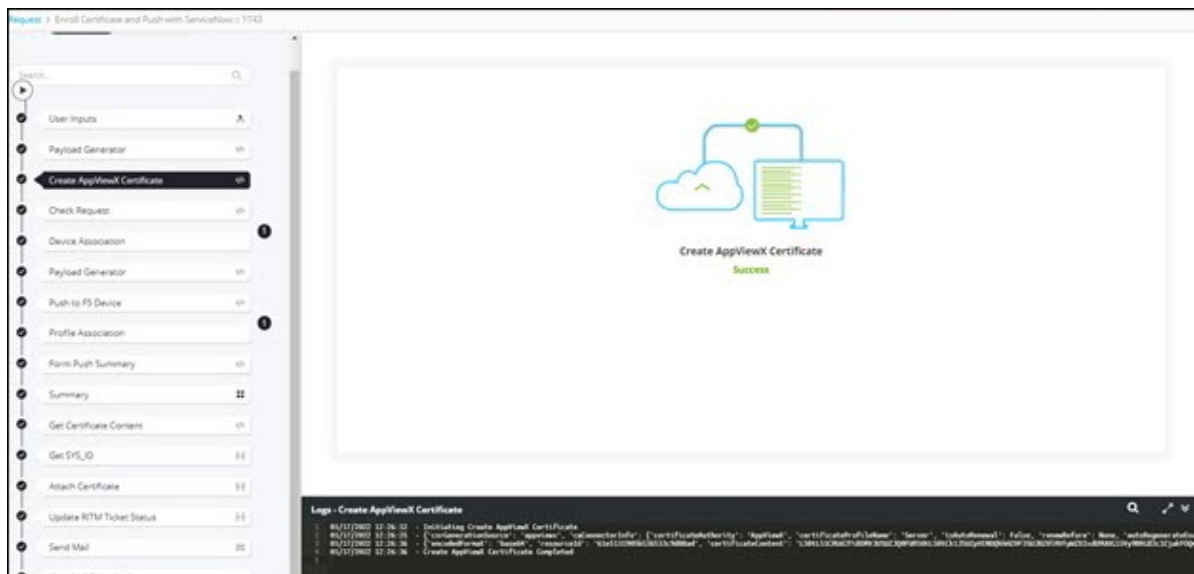
* ServiceNow Account

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

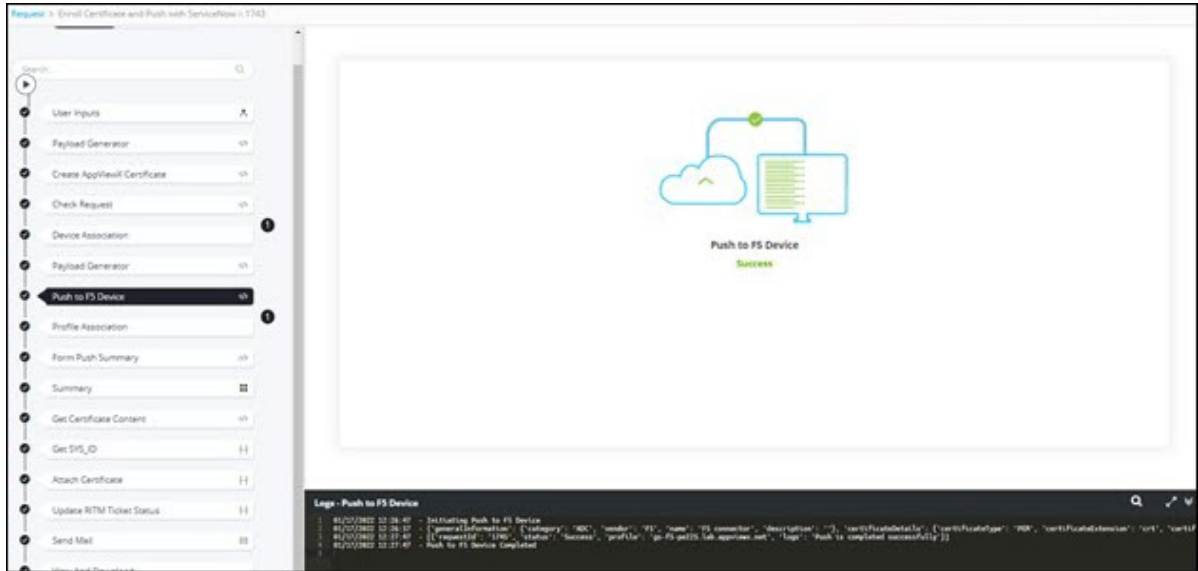


27. Click **Submit**.

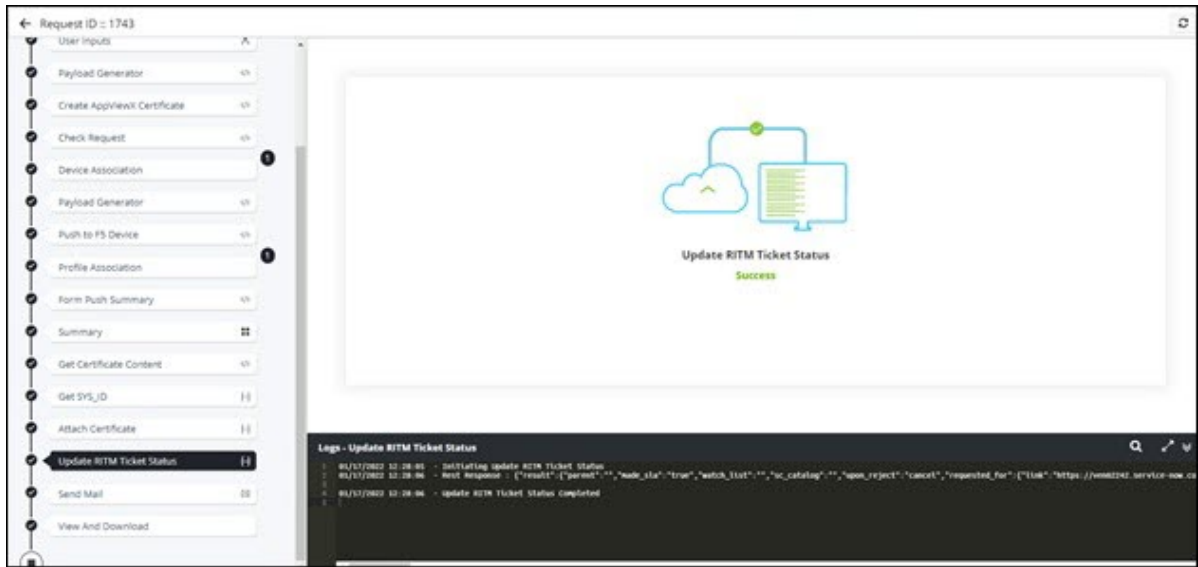
- AppViewX Certificate is created successfully.



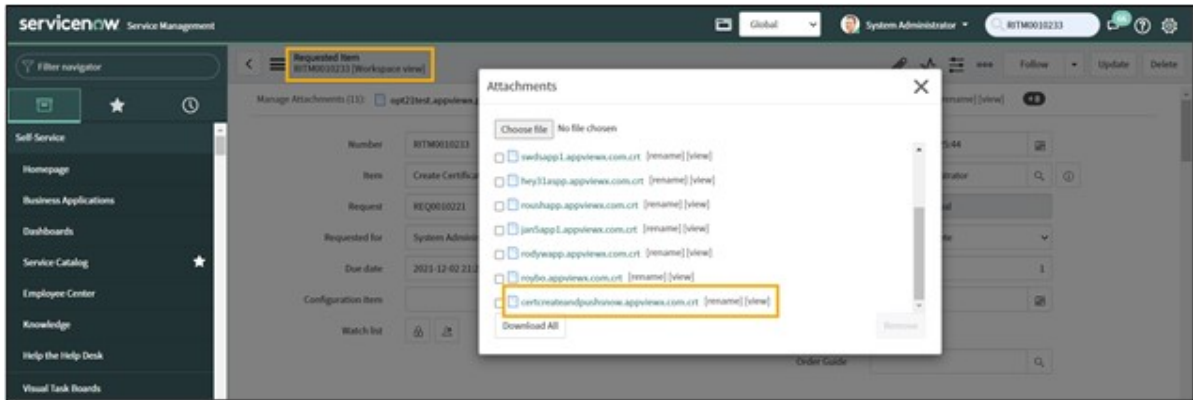
- Certificate is pushed to the selected device.



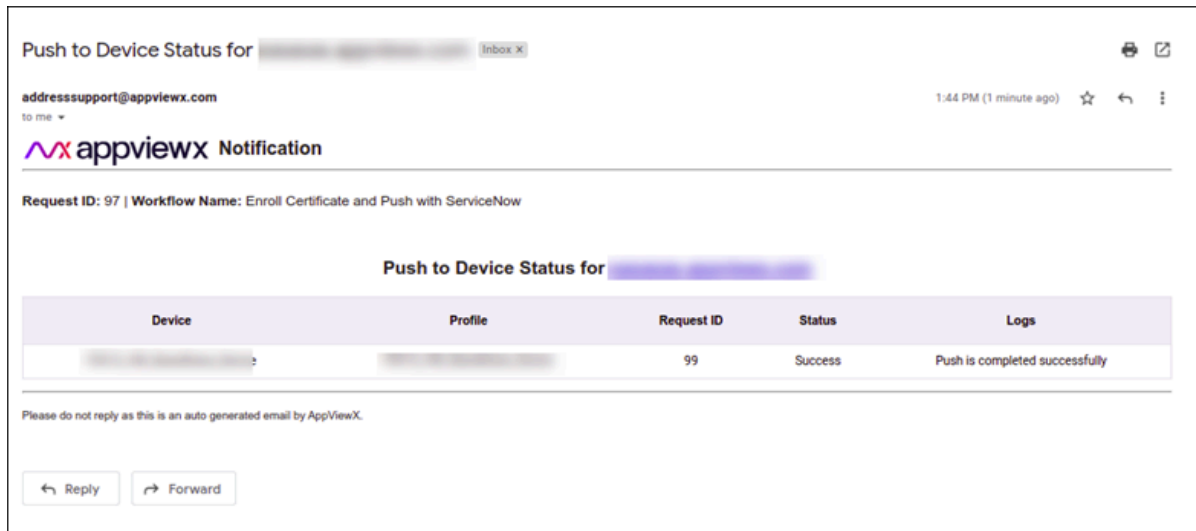
- RITM ticket status updated.



- 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.

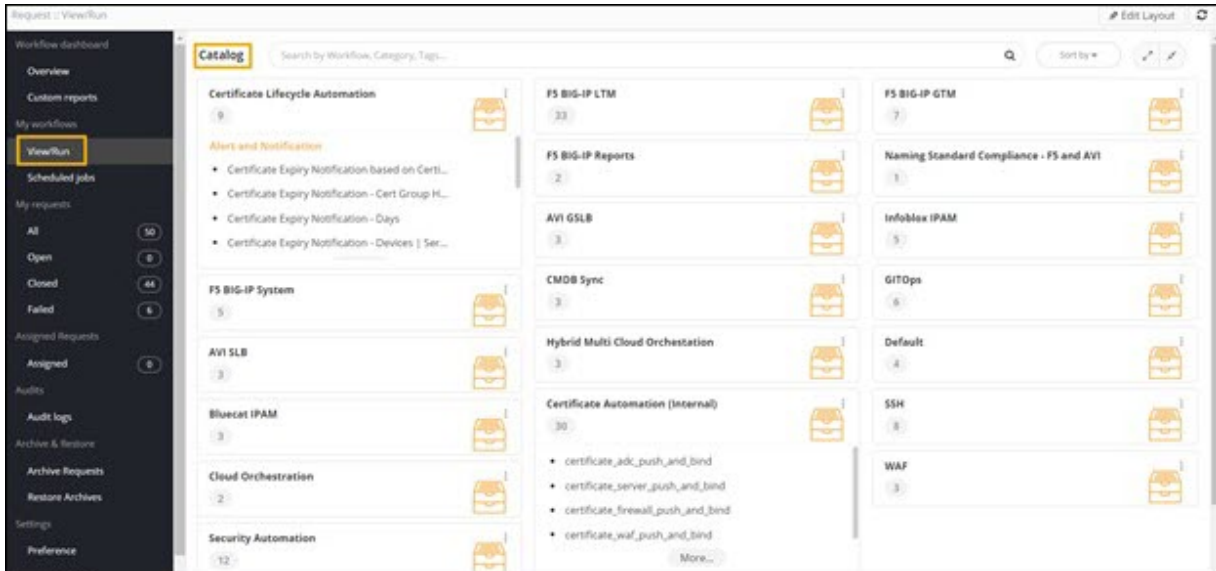




Easy Certificate Provisioning

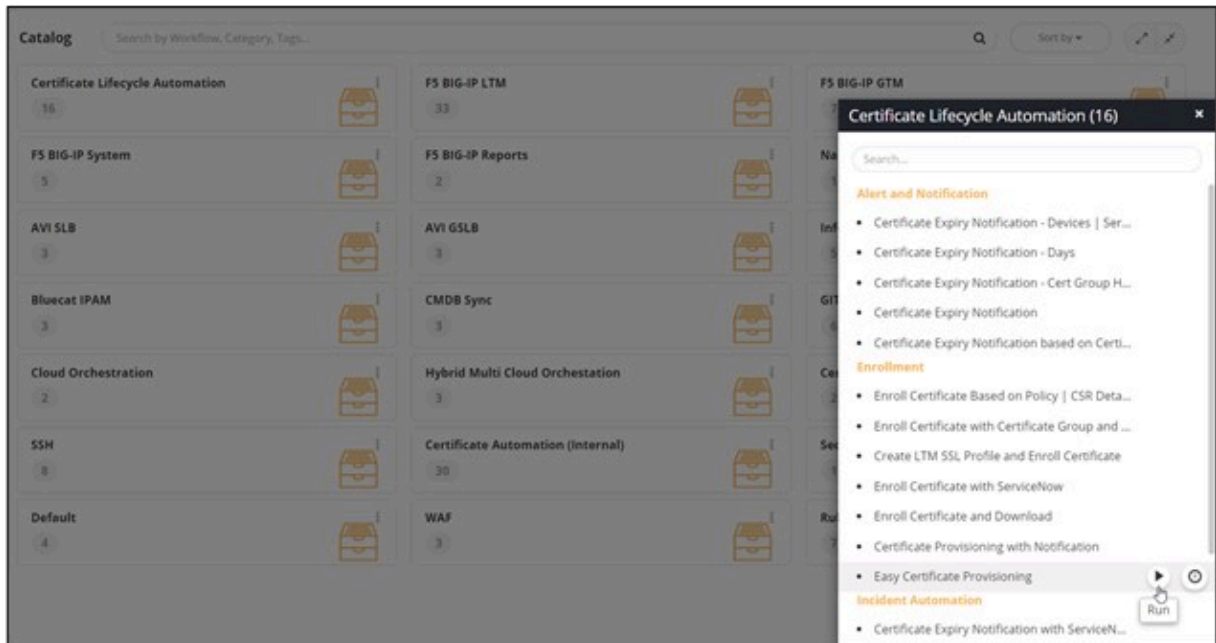
This workflow allows you to create an AppViewX certificate and push to a device available in the instance. Once the certificate is created, an email is sent to the logged in user informing them about the Push to Device Status of the certificate.

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  .



i **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**.



i **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.

Device Details

* Device Type:

* Vendor:

* Device:

* Linux Actions:


* Profiles/Application:





* KDB Password:

* Push to Devices

Search...

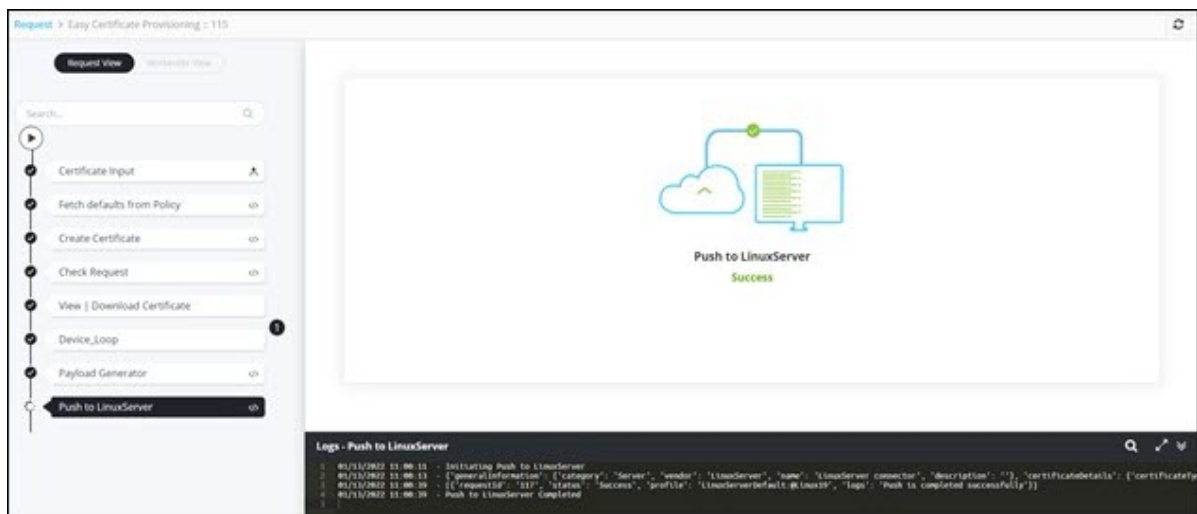
<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****

 **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.

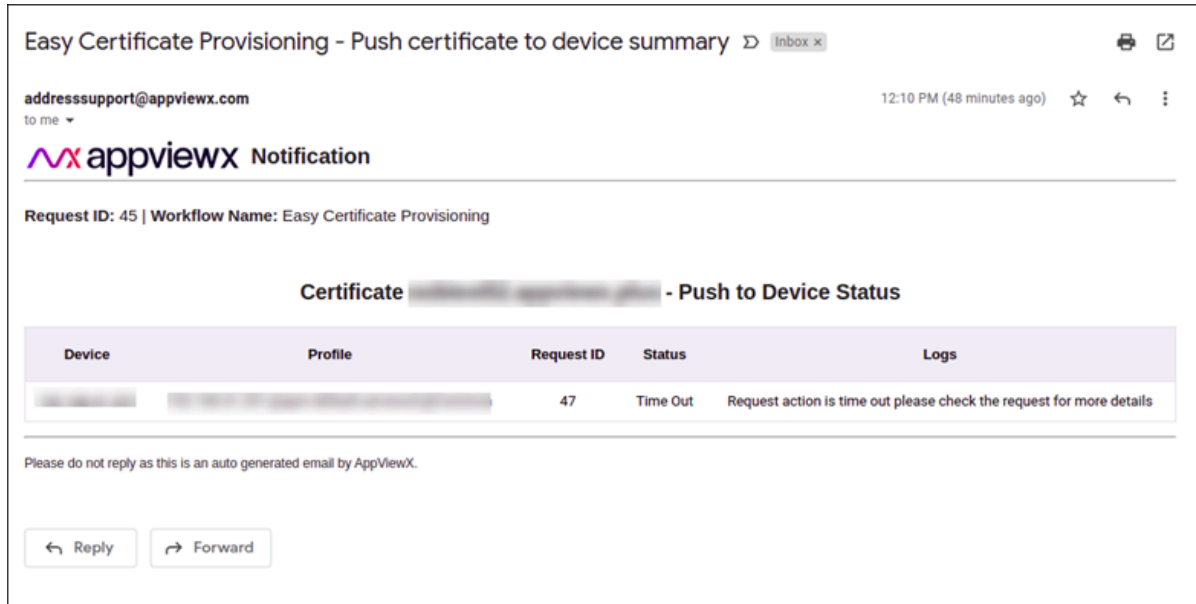



- Push to Device Status **Summary** displayed.

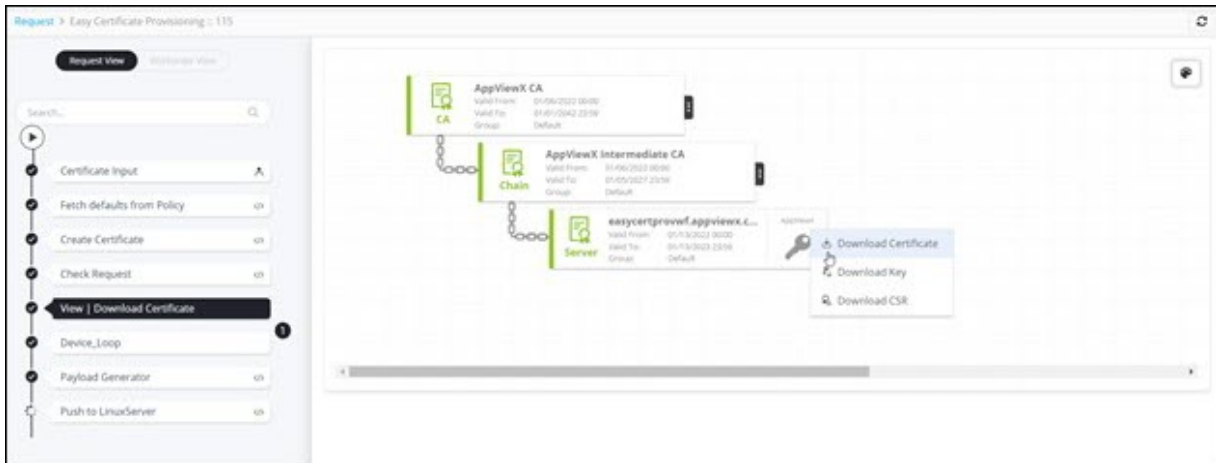


 **Note:** To download the Push to Device Status Summary, from the top right corner of the screen, click  .

- 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.

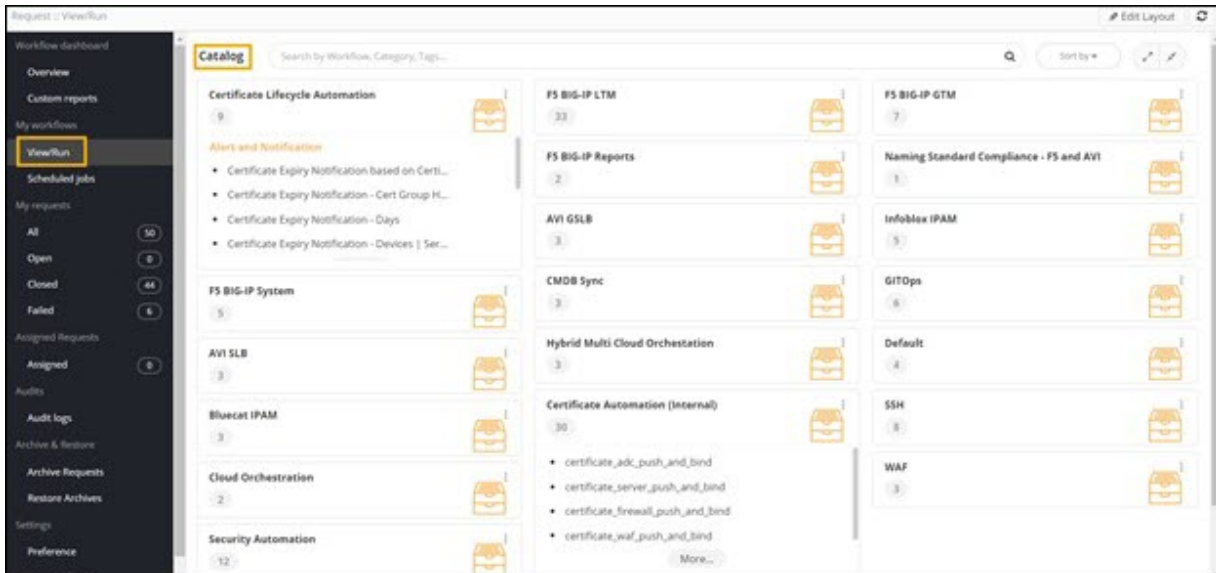


Enroll Certificate with CAA Validation


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

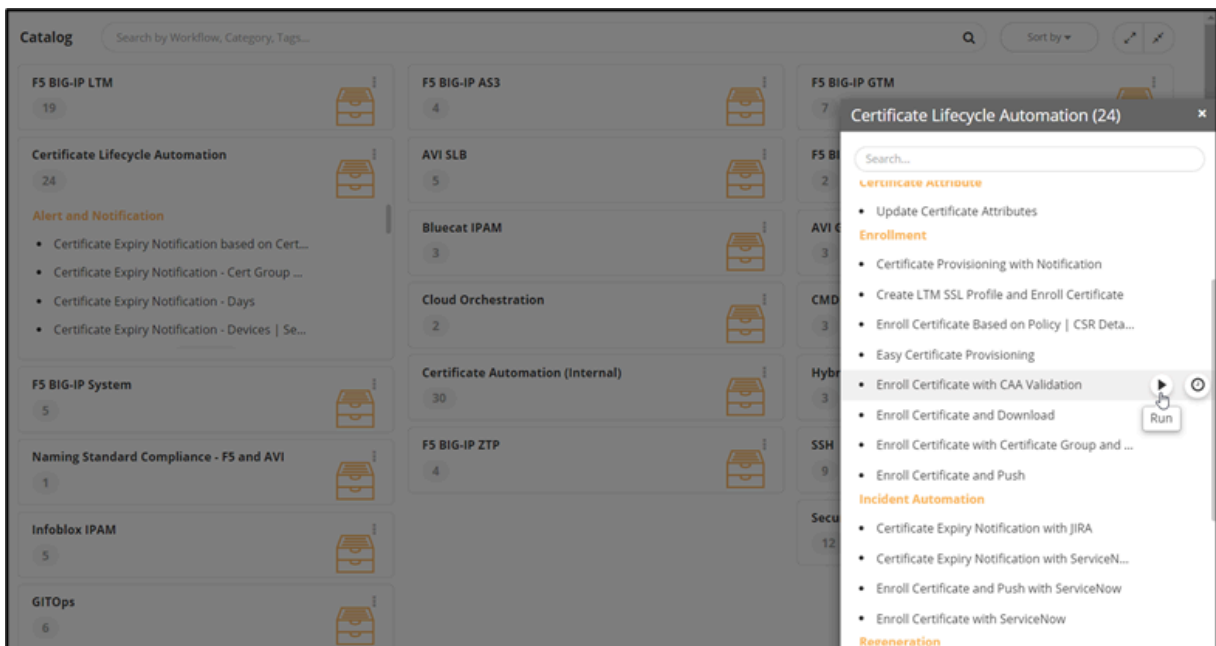
To trigger this workflow:

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 .



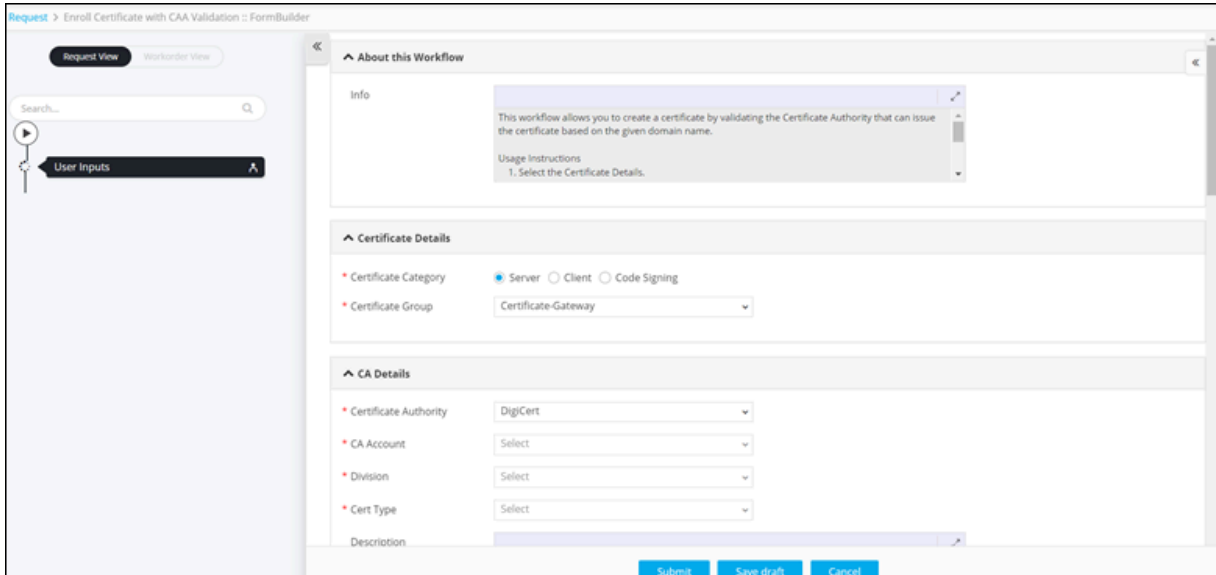
3. From the options displayed, select **Full View**.

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

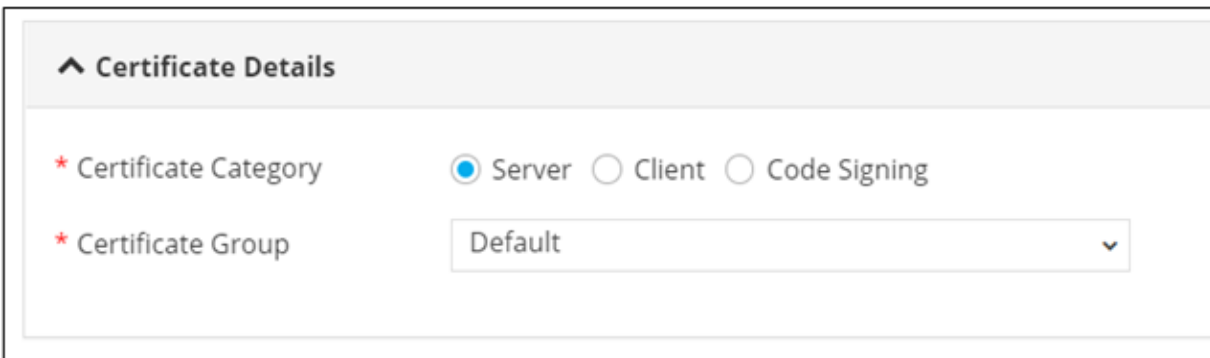


Tip: You can also search for the workflow by typing the workflow name in the search bar.


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: <ul style="list-style-type: none"> • Server • Client • Code Signing <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Server is the default selection. </div>
* 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.

^ CA Details

* Certificate Authority



* CA Account



* Division

* Cert Type

Description

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

Field	Description
* Certificate Authority	<p>Select the Certificate Authority from the available options:</p> <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> Note: This list will be populated based on the Certificate Group selected in the Certificate Details section.</p> </div>
* CA Account	<p>Select the CA Account from the options available in the dropdown.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> Note: This field is populated based on the CA selected.</p> </div>
* Division	<p>Select the Division from the options available in the dropdown.</p>

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.

^ CSR Parameters

* Common Name ⓘ

Subject Alternative Name ▼

DNS ⓘ

IP Address ⓘ

Organization

Organization Unit

Locality

State

Country

Email Address

* Validity Unit ▼

* Validity Value ▼


* Key Type ▼

* Bit Length ▼

* Hash Function ▼

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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: This field is displayed only when DigiCert is selected as the Certificate Authority. </div>
Email Address	Enter the email address.
*Validity Unit	Select the validity unit as: <ul style="list-style-type: none"> • 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.

* Attribute

* Attribute Value

Certificate Attributes

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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 .

<input type="checkbox"/>	Attribute	Attribute Value
<input type="checkbox"/>	Department	itm
<input type="checkbox"/>	Department	dev
<input type="checkbox"/>	Department	engg

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.

^ Vendor Specific Details

* Server Type

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Ejbca Certificate Profile Name

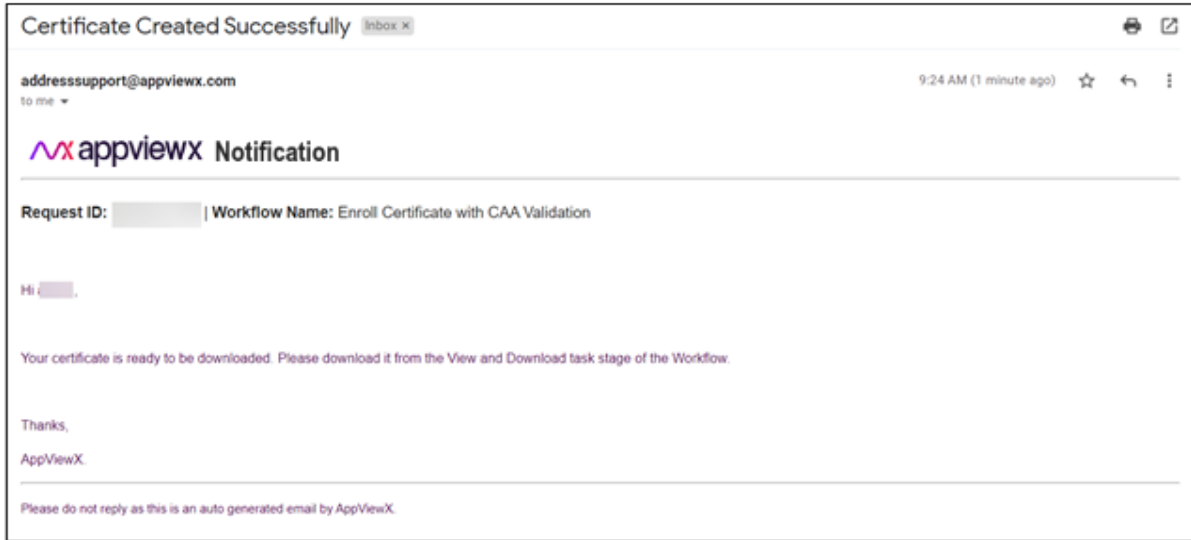


Note: The Vendor Specific Details section is displayed only when DigiCert or EJBCA is selected as the Certificate Authority under the CA Details section. The field(s) displayed will vary based on the CA selected.

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

^ Notifications

* Email ID ?



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**.

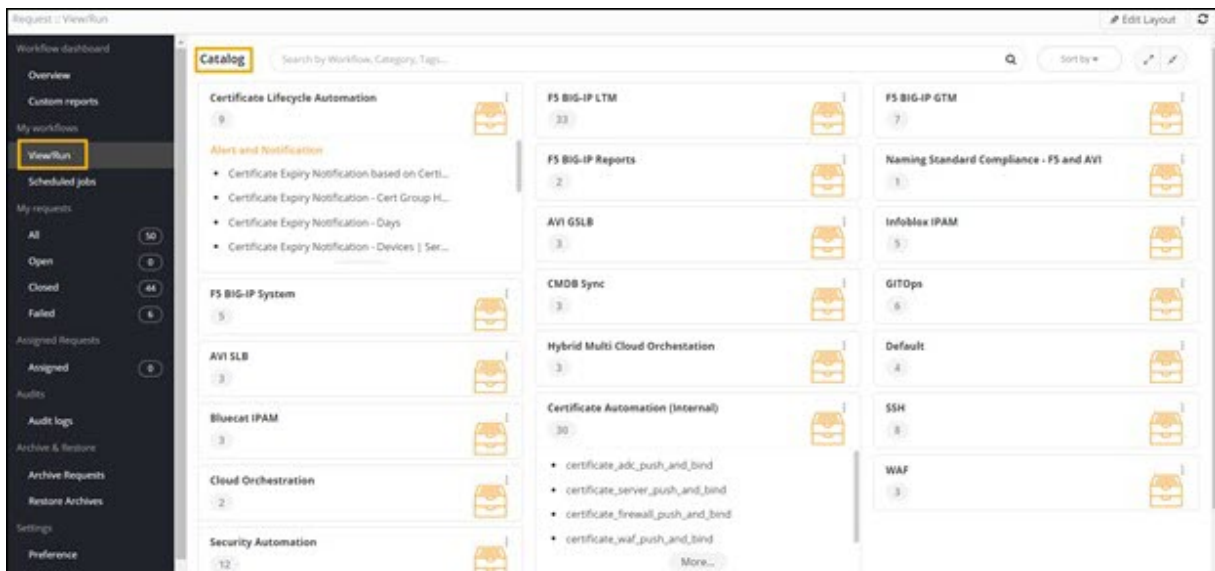


Enroll Certificate and Push


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

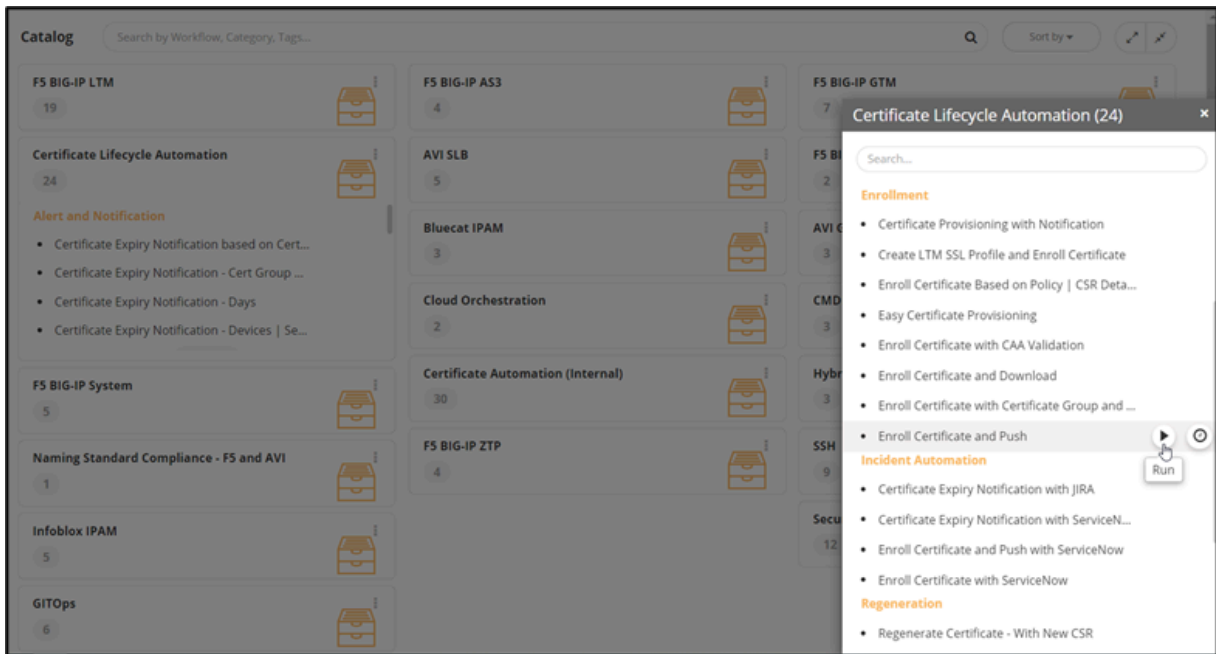
To trigger this workflow:


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



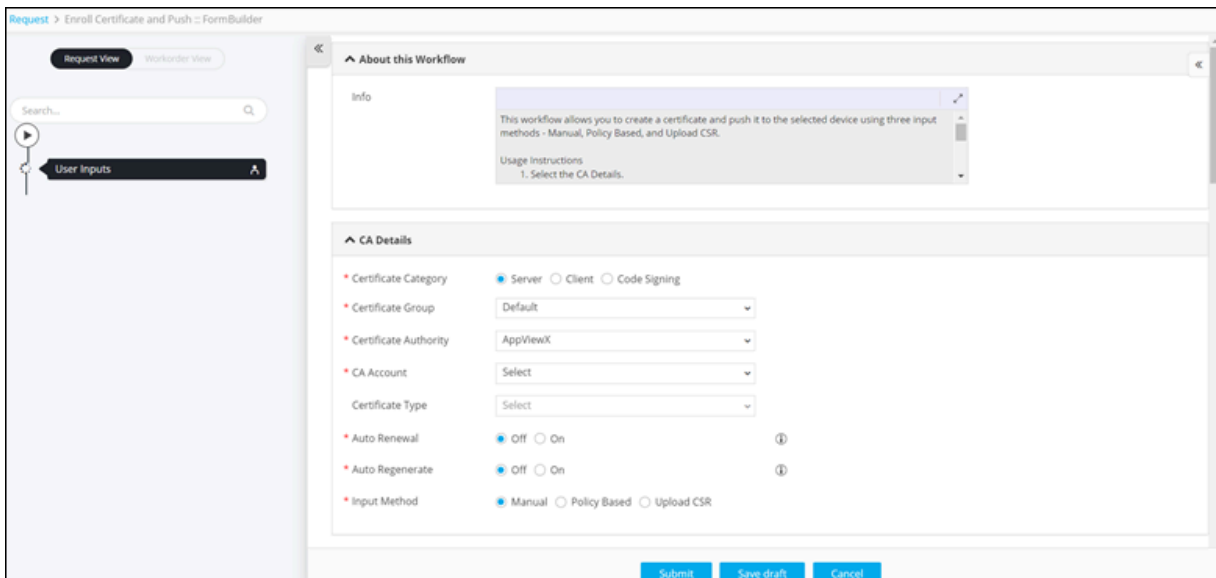
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click  .
3. From the options displayed, select **Full View**.

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:

^ CA Details

* Certificate Profile Server Client Code Signing

* Certificate Group

* Certificate Authority

* CA Account

* Division

Certificate Type








* Auto Renewal Off On i


* Auto Regenerate Off On i

* Input Method Manual Policy Based Upload CSR

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

Field	Description
* Certificate Profile	<p>Select the Certificate Profile from the following options:</p> <ul style="list-style-type: none"> • Server • Client • Code Signing <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p> Note: Server is the default selection.</p> </div>
* Certificate Group	Select the Certificate Group from the options available in the dropdown.
* Certificate Authority	<p>Select the Certificate Authority from the options available in the dropdown. The following CAs are supported:</p> <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA

Field	Description
	<ul style="list-style-type: none"> • Microsoft Enterprise • AppViewX <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the Certificate Group selected. </div>
*CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the Certificate Authority selected. </div>
*Division	Select the Division from the options available in the dropdown. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when Digicert is selected as the CA. </div>
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 . <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Default selection is set to Off. </div>
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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when the Auto Renewal field is enabled. </div>
*Auto Regenerate	Select the required radio button to enable/disable Auto Regenerate . <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Default selection is set to Off. </div>
Start Regenerating (Days)	Enter the number of days in the Start Regenerating (days) field. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when the Auto Regenerate field is enabled. </div>
*Input Method	Select the required Input Method . The options available are:

Field	Description
	<ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: Manual is the default selection. </div>
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 **CSR Parameters**, enter the field information as shown.


^ CSR Parameters

* Common Name	<input type="text" value="createandpush.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="createandpush.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text"/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
Challenge Password	
* Hash Function	SHA256
* Key Type	RSA
* Bit Length	2048

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>
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.

^ Certificate Attributes

* Attribute


* Attribute Value

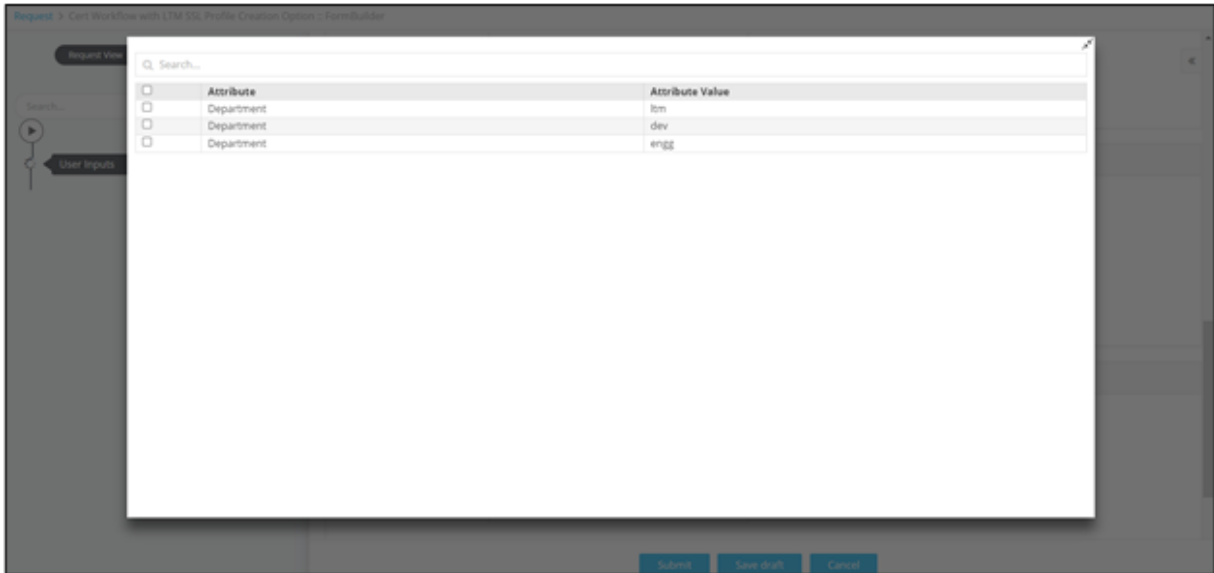
+
✎
↻
🗑

Certificate Attributes

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

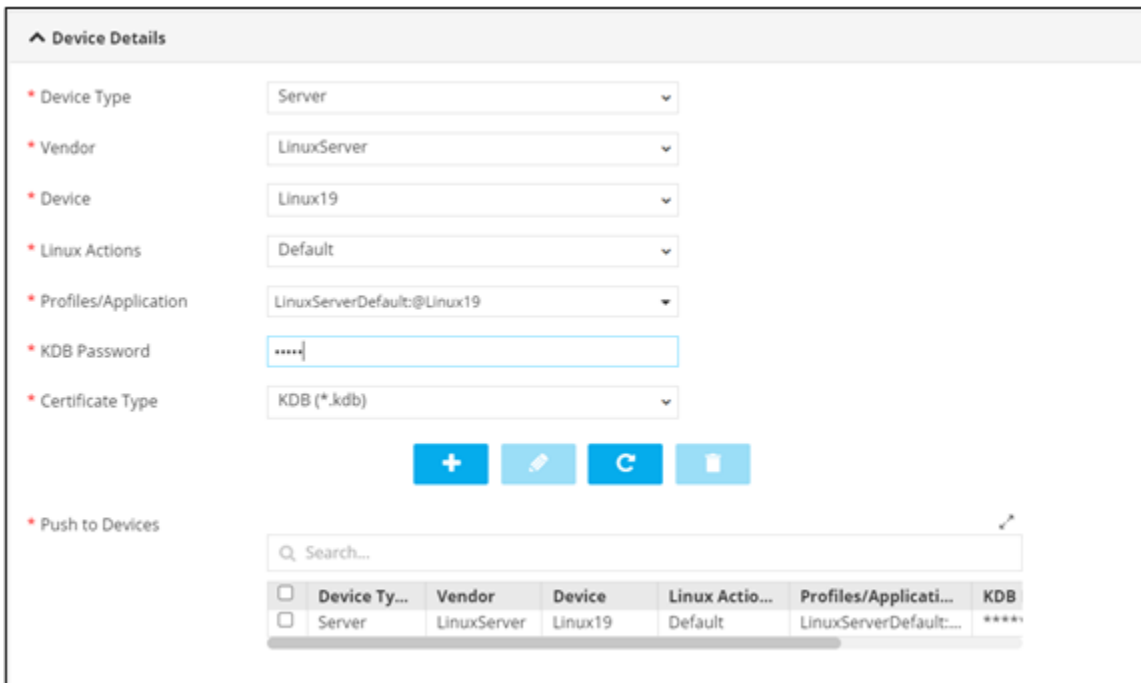
4. To add this attribute to the **Certificate Attributes** grid, click +.
5. To edit the value of a particular attribute, select the attribute in the grid and click ✎.
6. Enter the new value for the attribute in the **Value** field and click ✎ again to update the value.
7. To delete a certificate attribute,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

Device Information

* Device Type: Server

* Vendor: LinuxServer

* Device: Linux19

* Linux Actions: Default

* Profiles/Application: LinuxServerDefault:@Linux19

* KDB Password:

+ ✎ ↻ 🗑

* Push to Devices

🔍 Search...

<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****







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.

* Push to Devices

🔍 Search...

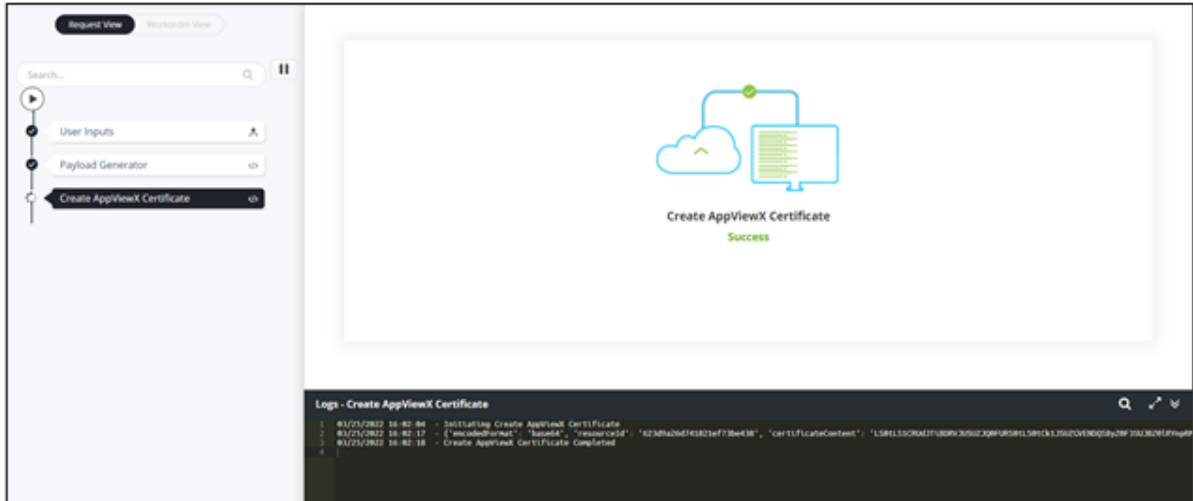
<input type="checkbox"/>	Vendor	Device	Linux Actions	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****

gs-f5-pe225.lab.appviewx.net,gs-f5-pe225.lab.appviewx.net:@KAN:@rrr,gs-f5-pe225.lab.appviewx.net:@NYC_test_vip_dont_delete_client_ssl:@Common

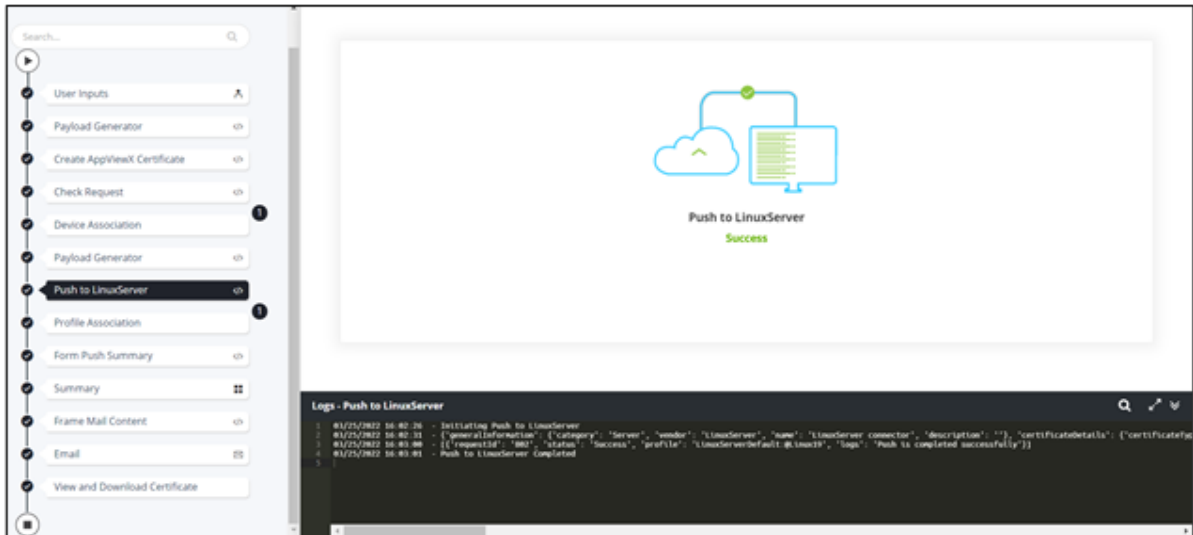
12. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
13. Select a new device and click  again to update the value.
14. To delete a profile/application, select the row to be deleted in the grid and click .
15. To maximize the **Push to 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**.

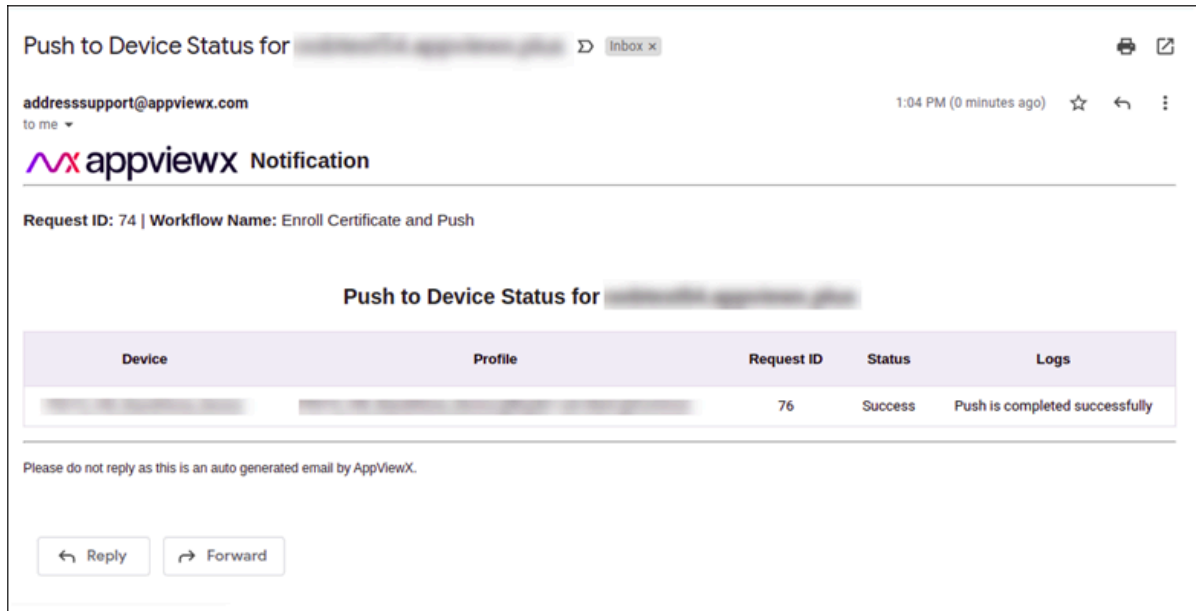
- Certificate created successfully.



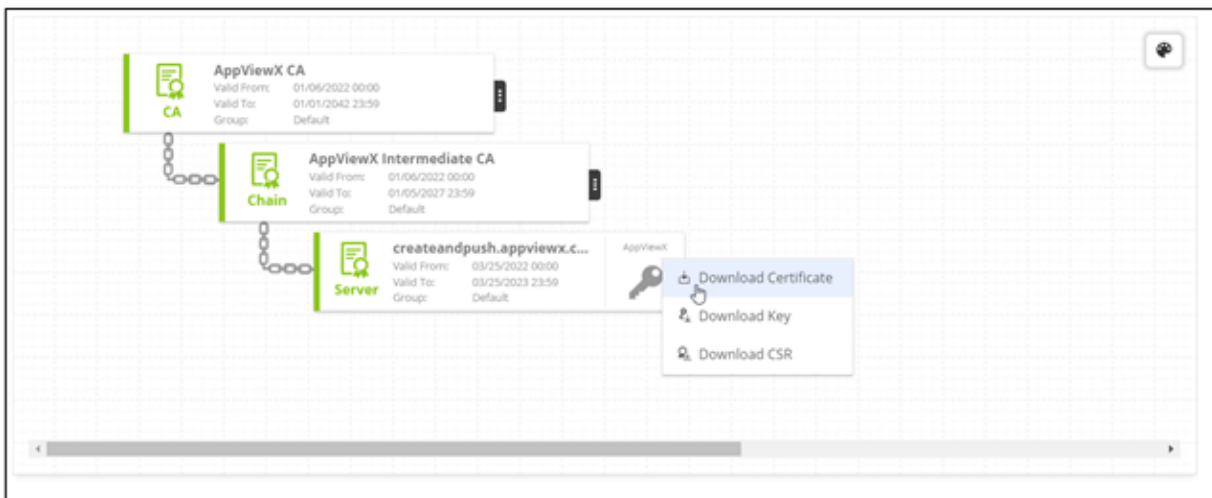
- Certificate pushed to Linux server successfully.



- 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**.

^ CSR Parameters		
* Common Name	<input type="text"/>	
Subject Alternative Name	DNS 	
DNS	<input type="text"/>	
IP Address	<input type="text"/>	
Organization	<input type="text"/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	Years 	
* Validity Value	1	

* Validity Unit	Years
* Validity Value	1
Challenge Password	
* Hash Function	SHA256
* Key Type	RSA
* Bit Length	2048



Note: For more information on the form fields, refer to the field information described in the [Manual](#) section.

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

^ Certificate Attributes

* Attribute: Department




* Attribute Value:


+ ✎ ↻ 🗑


Certificate Attributes

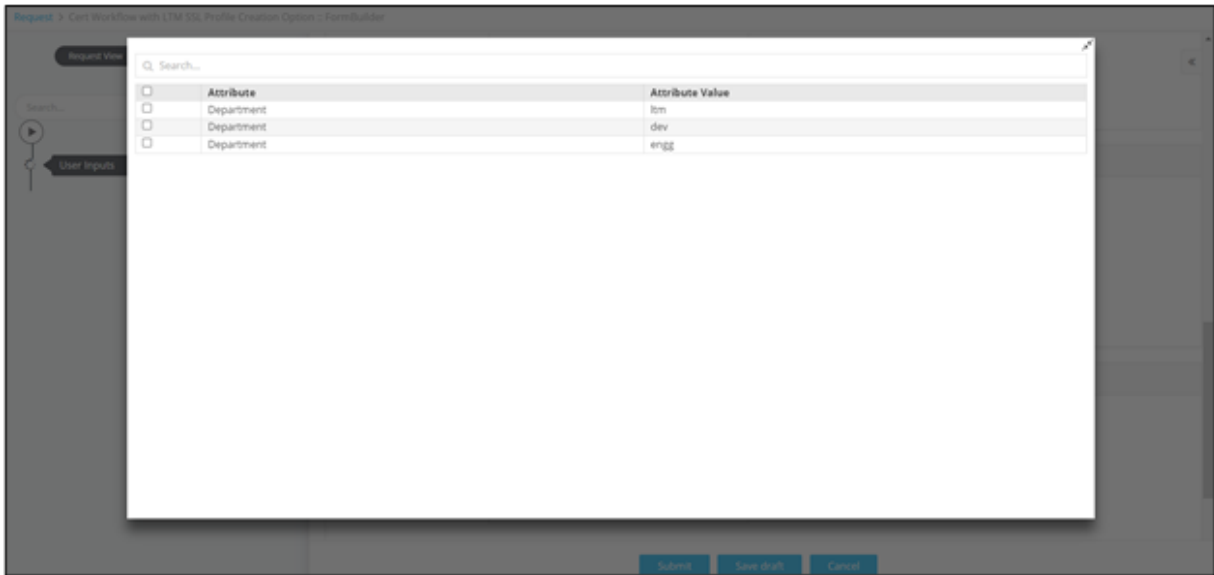
🔍 Search...

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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

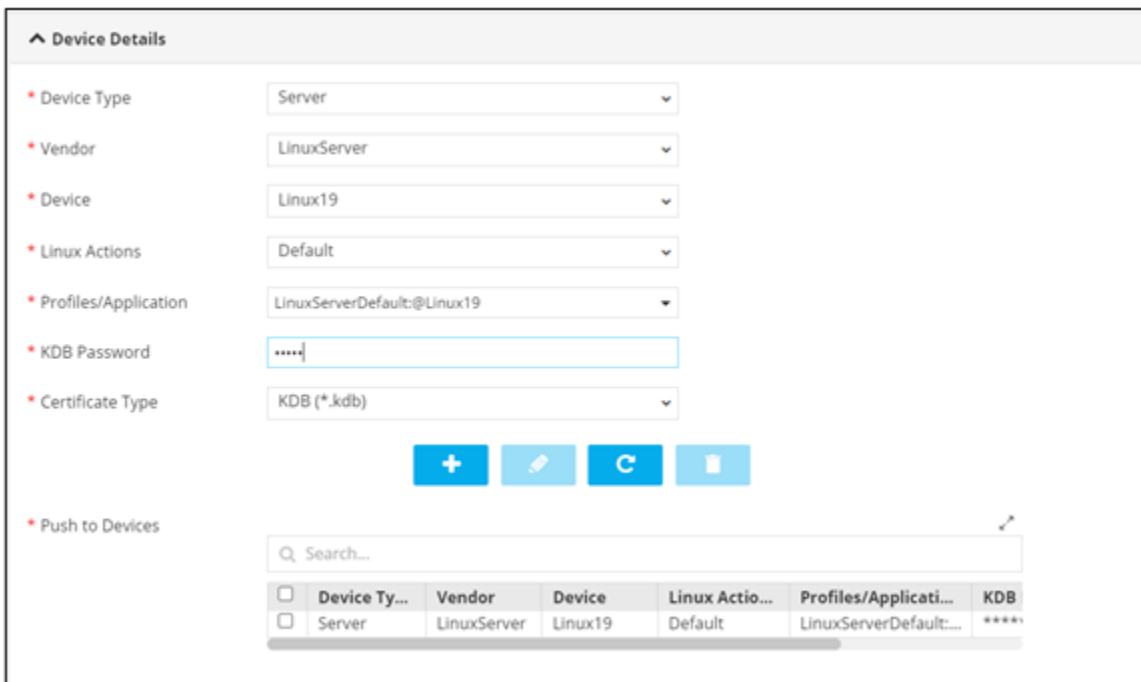
7. To delete a certificate attribute, select the attribute in the grid and click .

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.

Device Information

* Device Type: Server

* Vendor: LinuxServer

* Device: Linux19

* Linux Actions: Default

* Profiles/Application: LinuxServerDefault:@Linux19

* KDB Password:

+ ✎ ↻ 🗑️

* Push to Devices

🔍 Search...

<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****



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.

* Push to Devices

🔍 Search...

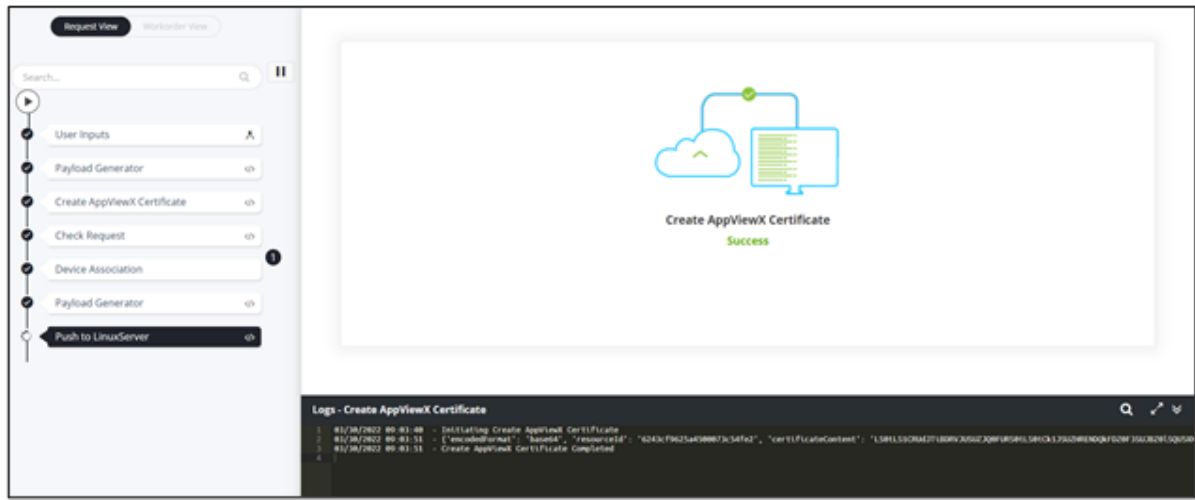
<input type="checkbox"/>	Vendor	Device	Linux Actions	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****

gs-f5-pe225.lab.appviewx.net,gs-f5-pe225.lab.appviewx.net:@KAN:@rrr,gs-f5-pe225.lab.appviewx.net:@NYC_test_vip_dont_delete_client_ssl:@Common

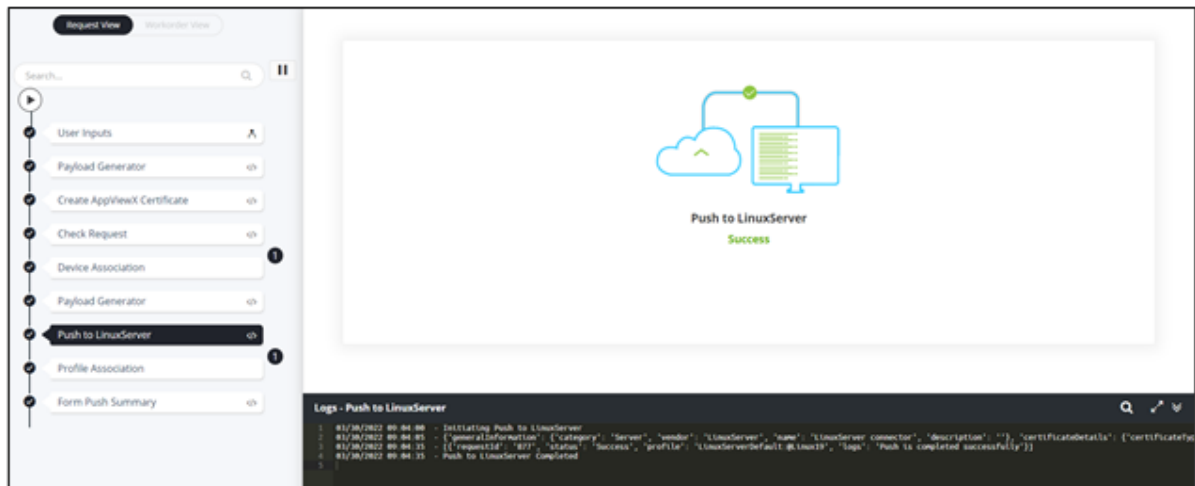
12. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
13. Select a new device and click again to update the value.
14. To delete a profile/application, select the row to be deleted in the grid and click .
15. To maximize the **Push to Devices** 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**.

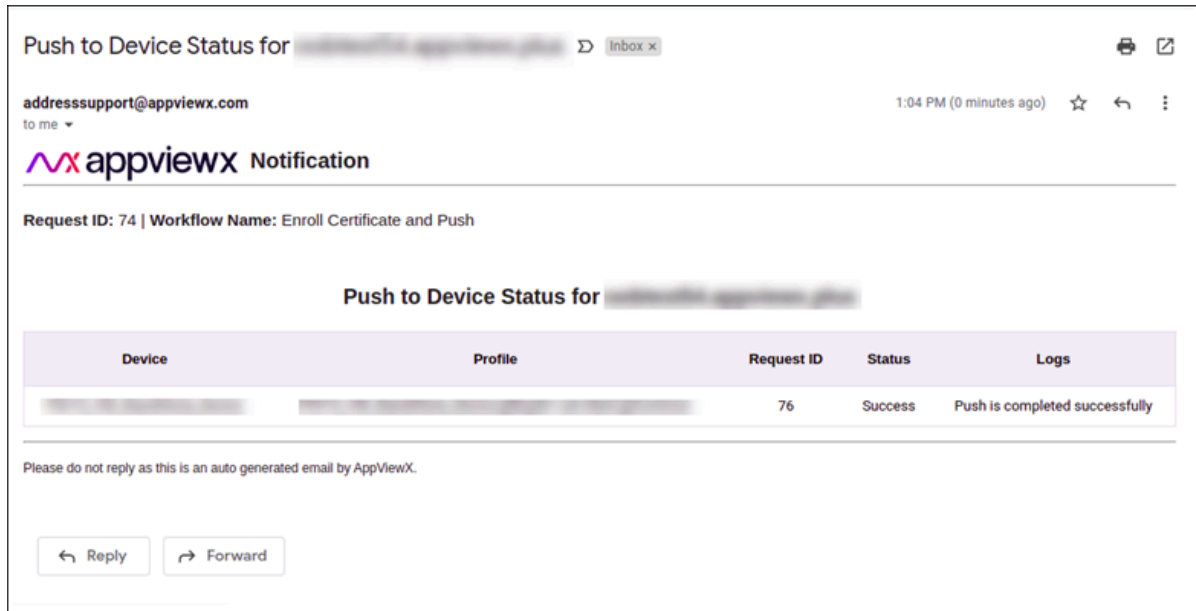
- Certificate created successfully.



- 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 .

The screenshot shows the "CSR Parameters" section. Under the "Upload CSR" heading, there is a text area containing the following CSR request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICFTCCAX4CAQAwgYYxIDAeBgNVBAMMF2RibW9nZW5jc3luYXBwdmld3guY29t
MRwwGgYDVQQQLDBNQcm9kdWN0IEVuz2luZWVyaW5nMRYwFAYDVQQKDA1BcHBWwV3
WCBJbmMuMRlwEAYDVQQHDAITYW4gRGlZ28xCzAJBgNVBAGMAkNBMQswCQYDVQQG
EwjVUzCBnzANBgkqhkiG9w0BAQEFAAOBJQAwgYkCgYEAzBf/pmFwq3PpeHM6bL9E
```

Below the text area is a blue button labeled "Fetch CSR Parameters".

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.

* Attribute: Department
 * Attribute Value:

Certificate Attributes

Attribute	Attribute Value
No records found	

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



Attribute	Attribute Value
Department	itm
Department	dev
Department	eng

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

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.

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.

Device Information

* Device Type:

* Vendor:

* Device:

* Linux Actions:


* Profiles/Application:

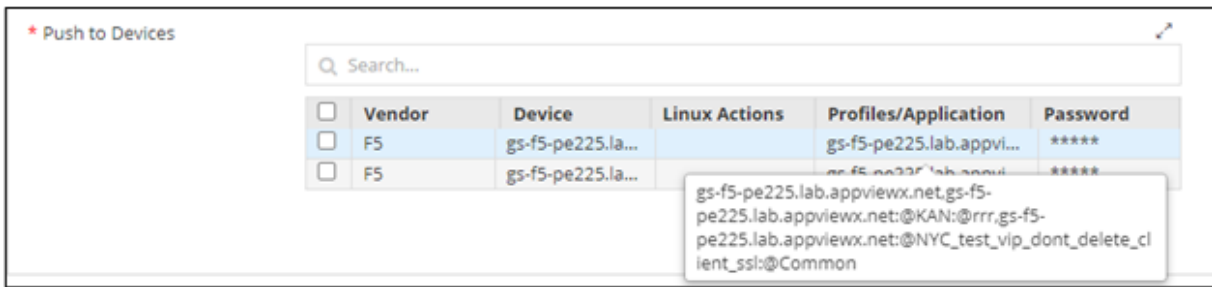
* KDB Password:





* Push to Devices

Search...

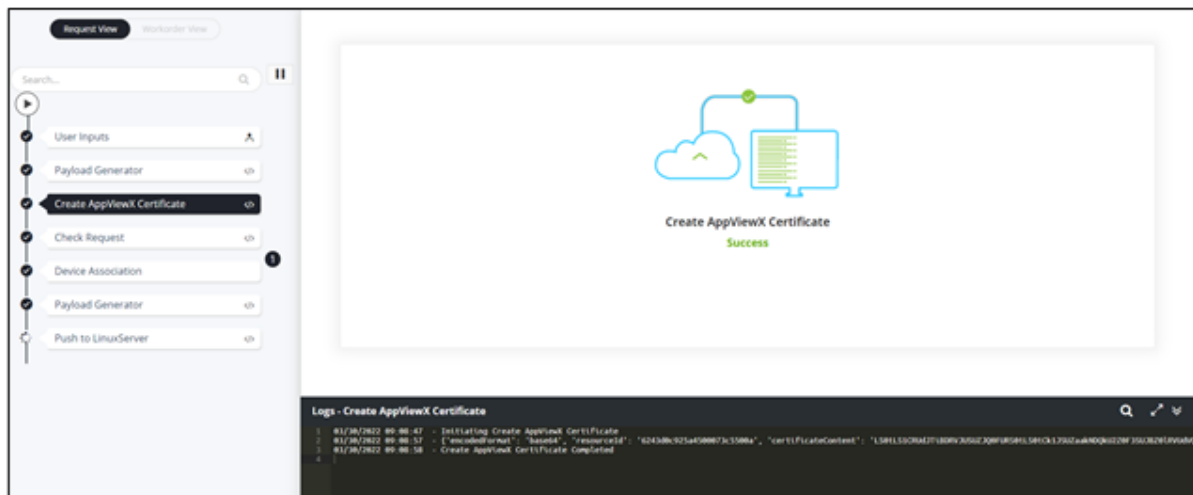
<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****

 **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.

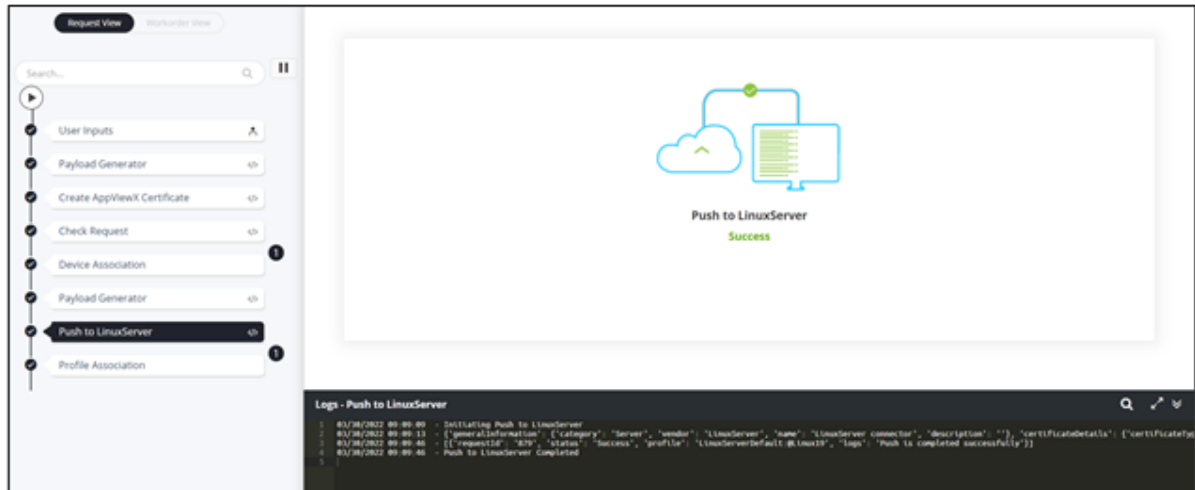


13. To edit the device details in the **Push to Devices** grid, select the row, modify the device details, and click .
14. Select a new device and click  again to update the value.
15. To maximize the **Push to Devices** grid, from the top right corner of the grid, click .
16. To delete a profile/application, 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**.

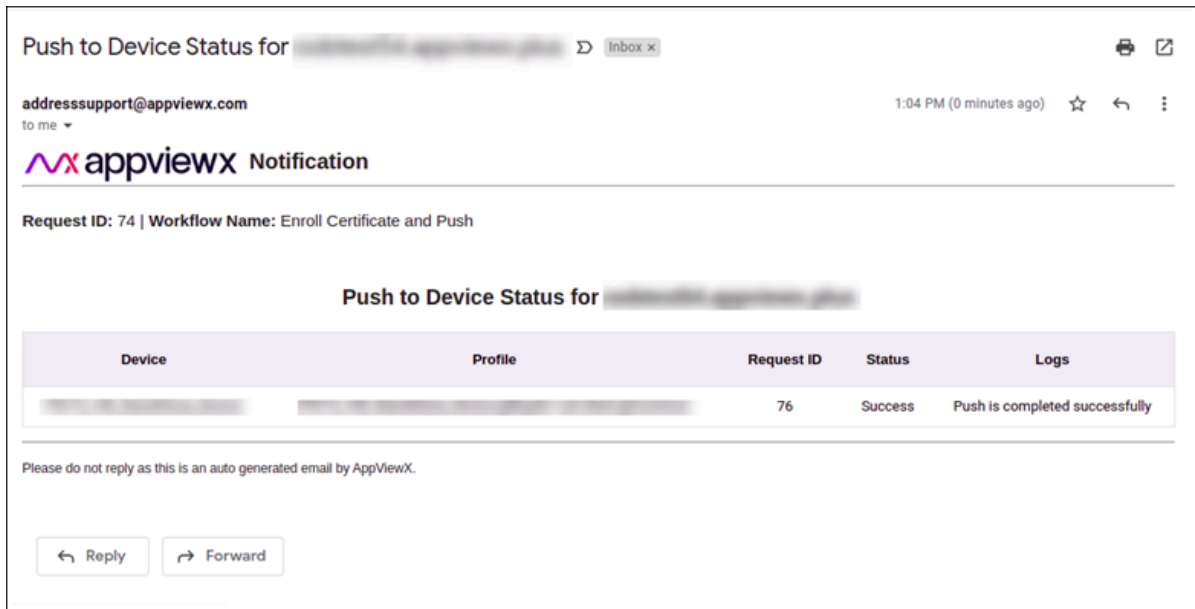
- Certificate created successfully.



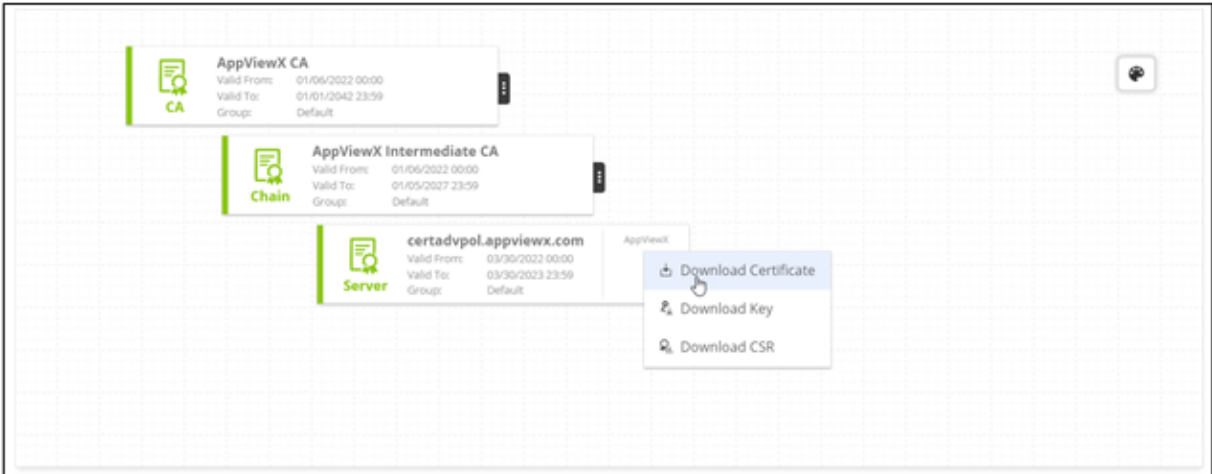
- Certificate pushed to Linux server successfully.



- 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
- Renew Certificate
- Regenerate Certificate with New CSR
- Renew Certificate and Push
- Renew Certificate with ServiceNow
- Renew Certificate and Push with ServiceNow

Overview

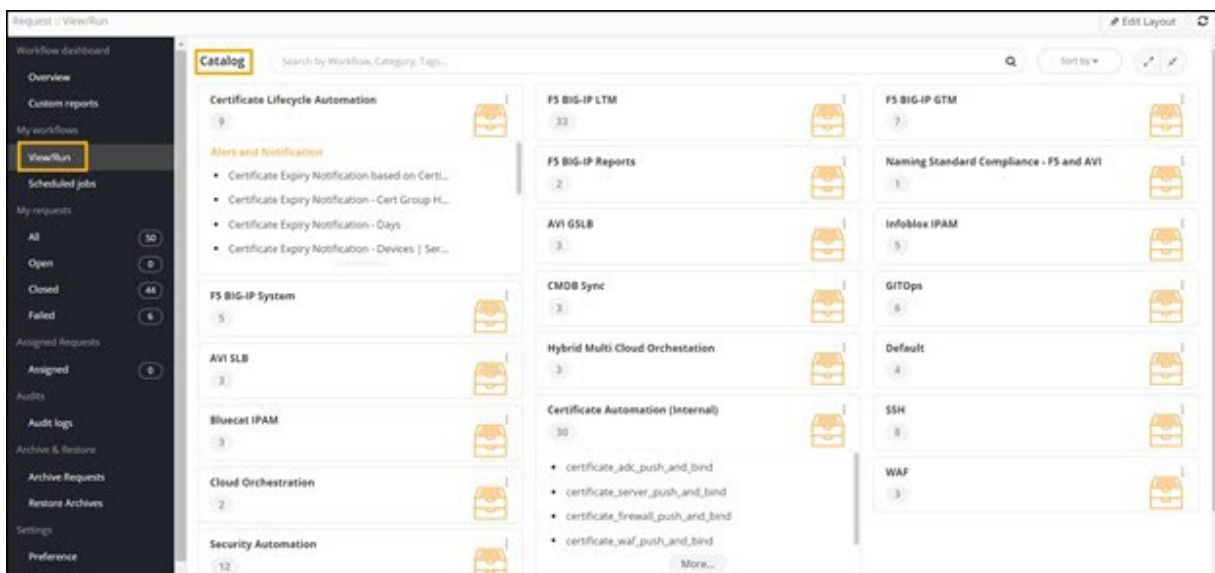
This section lists and describes the workflows that can be used to renew and regenerate certificates and push them to selected device(s) using the configured Certificate Authorities. Some workflows also describe Certificate Renewal with Incident Automation.

Renew Certificate

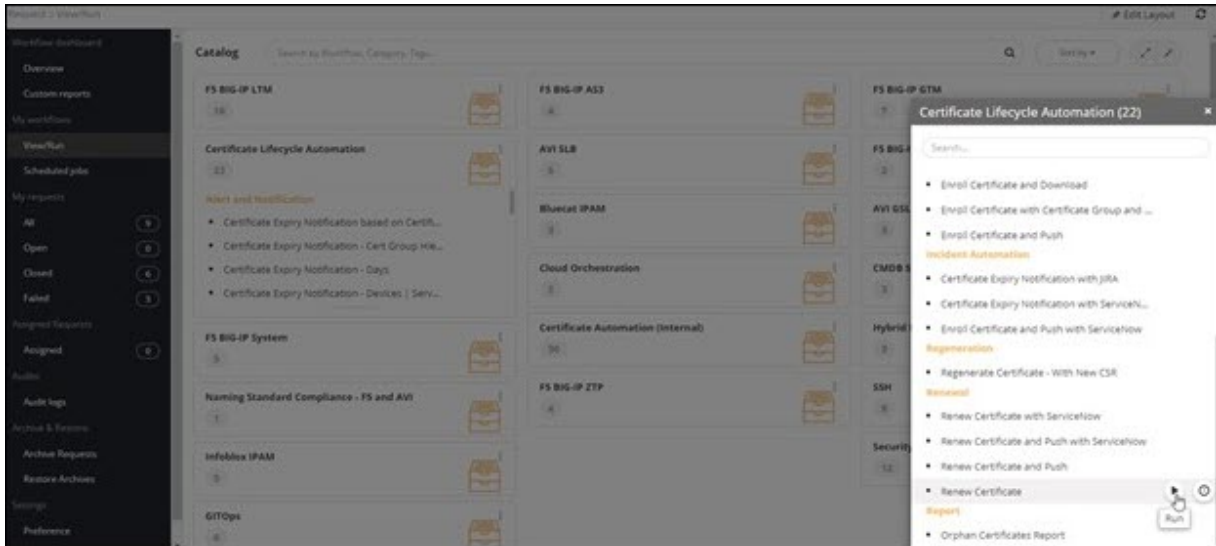
This workflow allows you to renew a certificate based on the certificate group and certificate authority.


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.

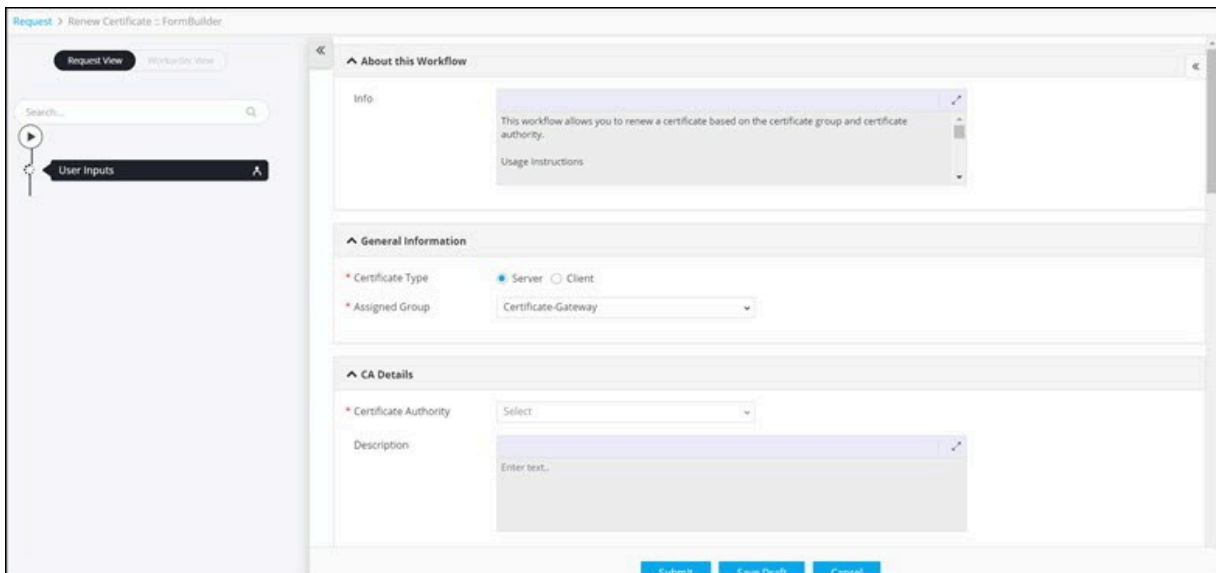


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** catalog, under the **Renewal** category, hover your mouse over the **Renew Certificate** workflow and click .

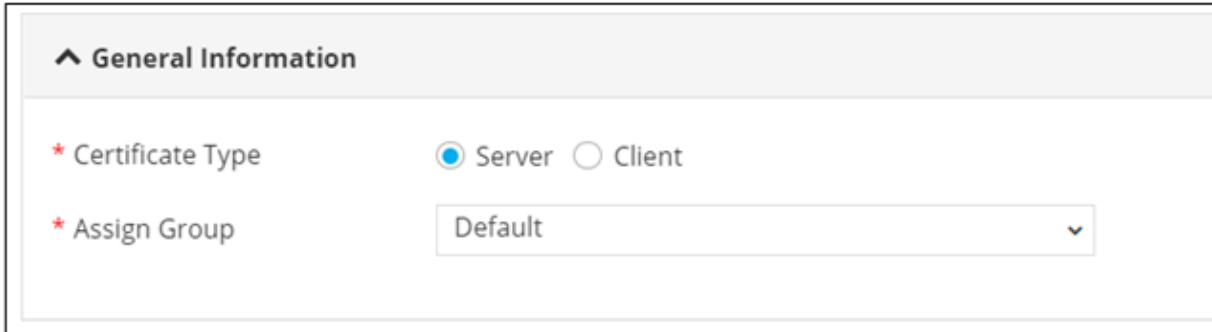


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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).



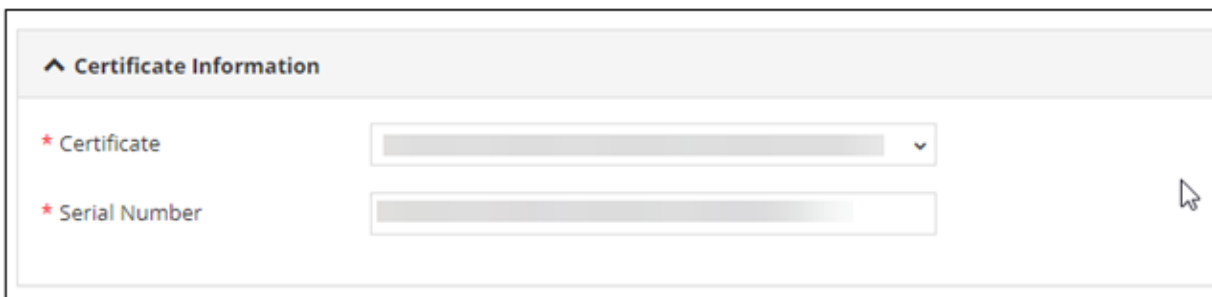
The screenshot shows the 'General Information' section of a form. It has a header with an upward-pointing arrow and the text 'General Information'. Below the header, there are two mandatory fields, each marked with a red asterisk. The first field is 'Certificate Type', which has two radio button options: 'Server' (which is selected) and 'Client'. The second field is 'Assign Group', which is a dropdown menu currently showing 'Default'.

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).



The screenshot shows the 'CA Details' section of a form. It has a header with an upward-pointing arrow and the text 'CA Details'. Below the header, there are two fields. The first is 'Certificate Authority', a dropdown menu with 'AppViewX' selected. The second is 'Description', which is a text area with a placeholder 'Enter text..' and a small icon in the top right corner.

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.



The screenshot shows the 'Certificate Information' section of a form. It has a header with an upward-pointing arrow and the text 'Certificate Information'. Below the header, there are two mandatory fields, each marked with a red asterisk. The first is 'Certificate', a dropdown menu. The second is 'Serial Number', a text input field. A mouse cursor is visible over the right side of the 'Serial Number' field.

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


^ CSR Parameters

* Common Name	<input type="text" value="certoob"/>
Subject Alternative Name	<input type="text" value="DNS"/>
DNS	<input type="text" value="certoob"/>
IP Address	<input type="text"/>
Email Address	<input type="text"/>
Directory Name	<input type="text"/>
URL	<input type="text"/>
Other Name	<input type="text"/>
Registered ID	<input type="text"/>
Organisation	<input type="text"/>
Organisation Unit	<input type="text"/>
Country	<input type="text"/>
City	<input type="text"/>
State	<input type="text"/>

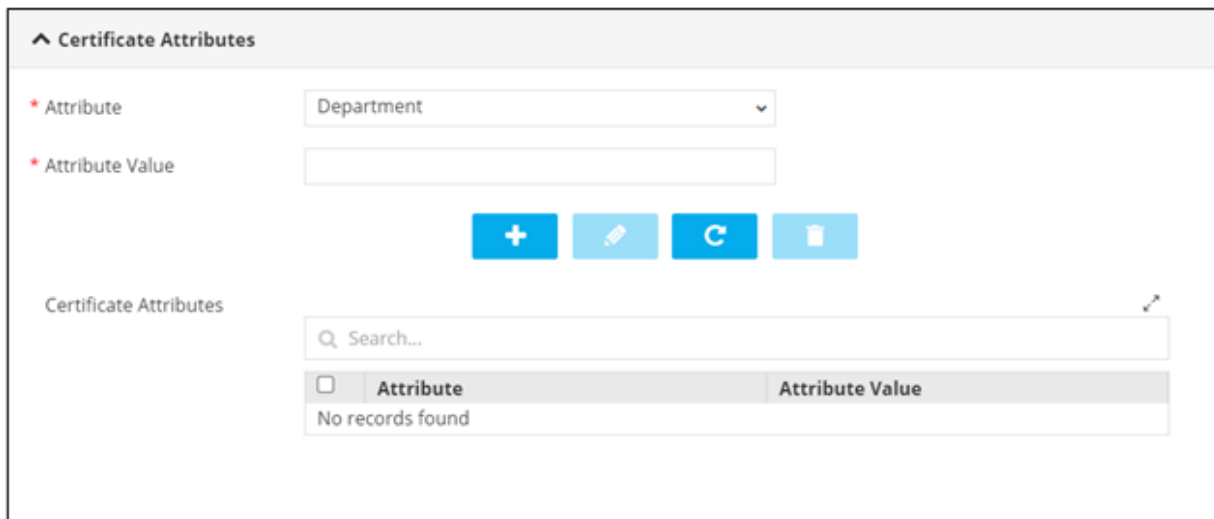
State	<input type="text"/>
Zip Code	<input type="text"/>
Email Address	<input type="text"/>
Validity Unit	Days <input type="button" value="v"/>
Validity Value	Select <input type="button" value="v"/>
* Hash Function	SHA256 <input type="button" value="v"/>
Bit Length	4096 <input type="text"/>
Key Type	RSA <input type="text"/>



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: <ul style="list-style-type: none"> • 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.

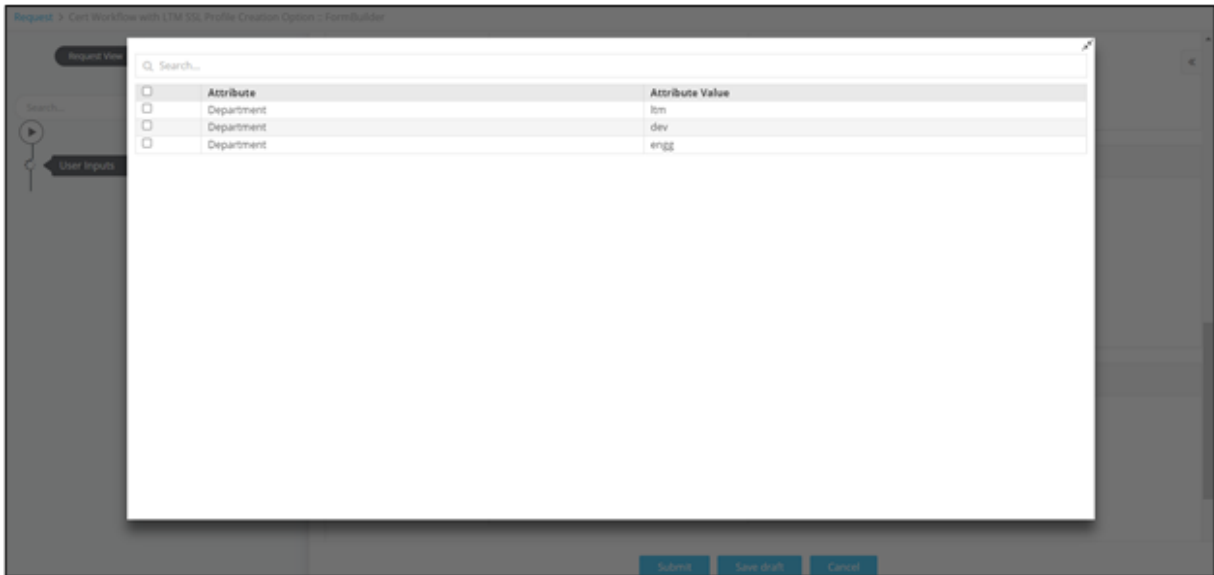
Field	Description
	 Note: This field is displayed only when DigiCert is selected as the Certificate Authority.
Email Address	Enter the email address.
*Validity Unit	Select the validity unit as: <ul style="list-style-type: none"> • Days • Months • Years
*Validity Value	Select a valid validity value.
*Key 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.

Vendor Specific Details

Order Id

* Server Type

Order valid from

Order valid till

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name

- When Entrust is selected as CA.

^ Vendor Specific Details

Additional Emails



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.

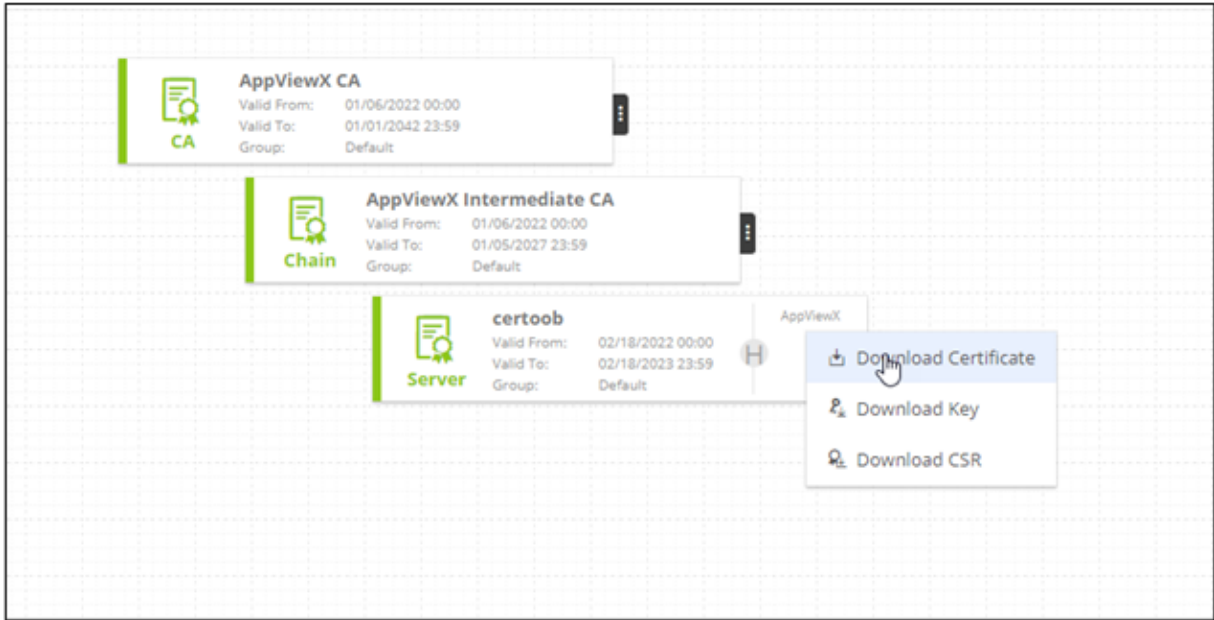
20. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

^ Notifications

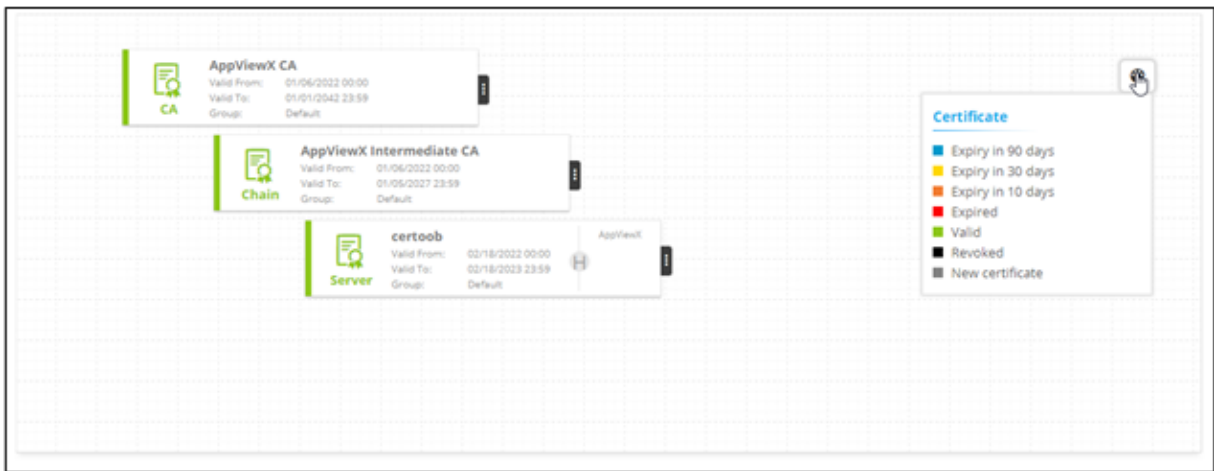
* Email ID i



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.



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

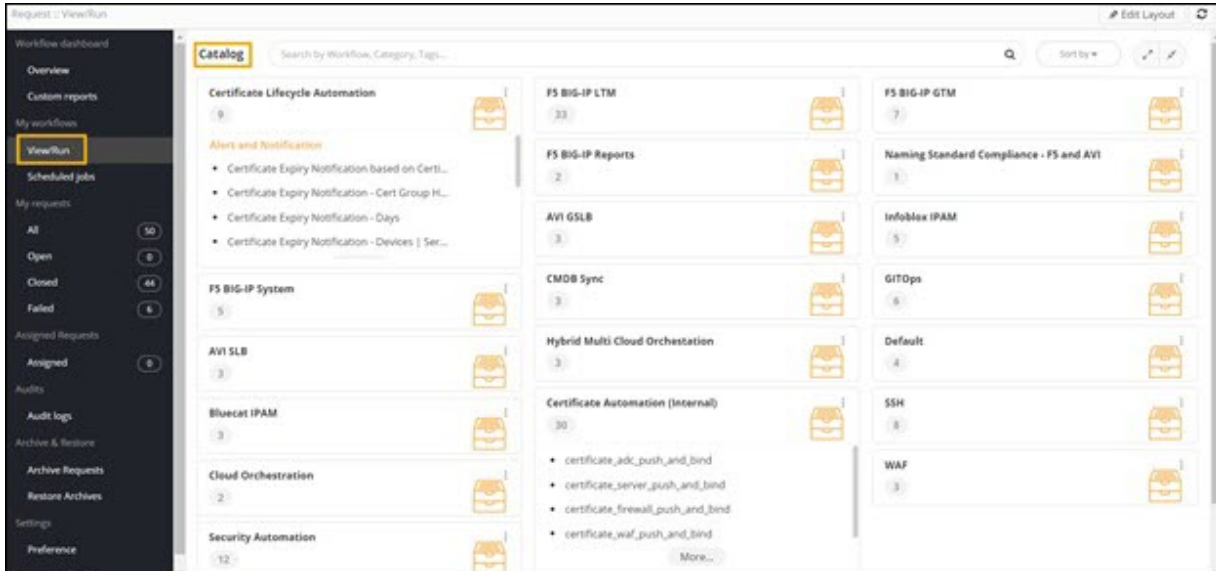




Regenerate Certificate with New CSR

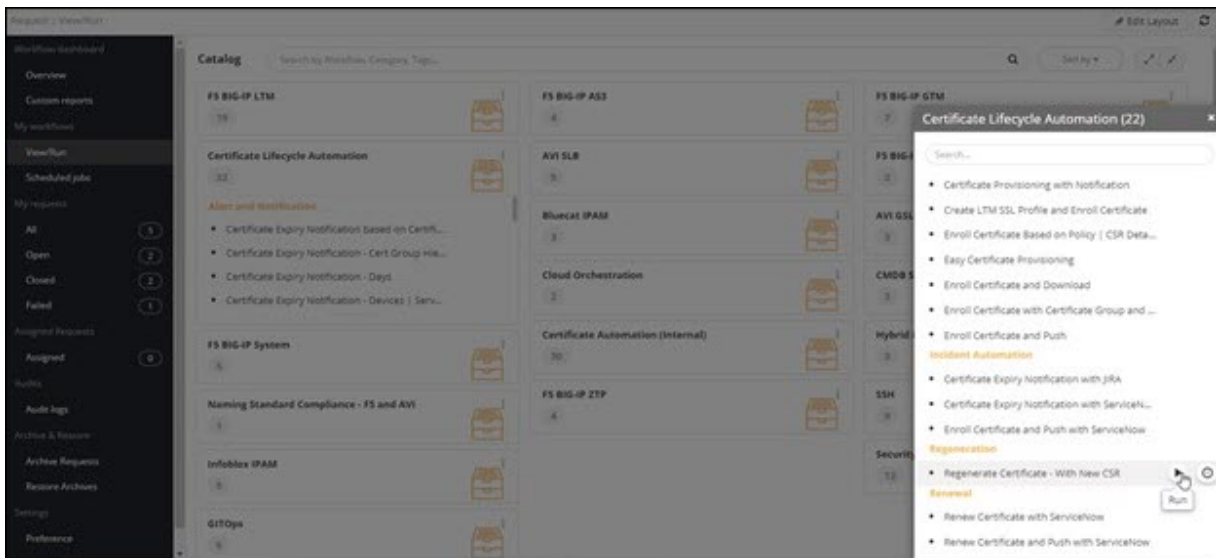
This workflow allows you to regenerate a certificate with a new CSR.


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: <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This list will be populated based on the Certificate Group selected in the Certificate Details section. </div>
* CA Account	Select the CA Account from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is populated based on the CA selected. </div>
* Division	Select the Division from the options available in the dropdown. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when DigiCert is selected as the CA. </div>
* 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](#)
- [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.

^ CSR Parameters		
* Common Name	<input type="text" value="certadvmanual.appviewx.com"/>	
Subject Alternative Name	<input type="text" value="DNS"/>	
DNS	<input type="text" value="certadvmanual.appviewx.com"/>	
IP Address	<input type="text"/>	
Organization	<input type="text" value="AppViewX Inc."/>	
Organization Unit	<input type="text"/>	
Locality	<input type="text"/>	
State	<input type="text"/>	
Country	<input type="text"/>	
Email Address	<input type="text"/>	
Zip Code	<input type="text"/>	
* Validity Unit	<input type="text" value="Years"/>	
* Validity Value	<input type="text" value="1"/>	

* Validity Unit	Years
* Validity Value	1
Challenge Password	
* Hash Function	SHA160
* Key Type	RSA
* Bit Length	Select





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

Field	Description
* Common Name	<p>Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: You have the option to change the common name of the regenerated certificate. </div>
Subject Alternative Name	<p>Select the SAN as either:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>
*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.

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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 .

<input type="checkbox"/>	Attribute	Attribute Value
<input type="checkbox"/>	Department	itm
<input type="checkbox"/>	Department	dev
<input type="checkbox"/>	Department	eng

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.

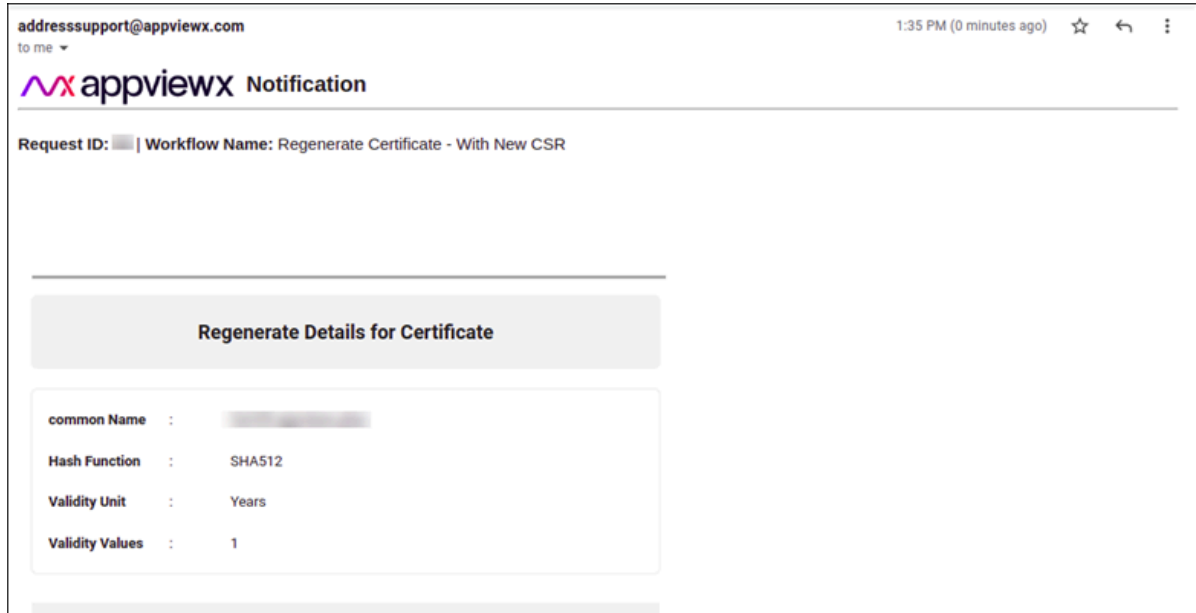
^ Vendor Specific Details	
Order Id	<input type="text"/>
* Server Type	Apache <input type="button" value="v"/>
Order valid from	<input type="text"/>
Order valid till	<input type="text"/>

- When EJBCA is selected as CA.

^ Vendor Specific Details	
* End Entity Profile Name	Select <input type="button" value="v"/>
End entity user name	<input type="text"/>
* Issuer Common Name	Select <input type="button" value="v"/>
* Certificate Profile Name	Select <input type="button" value="v"/>

- When Microsoft Enterprise is selected as CA.

^ Vendor Specific Details	
* Template Name	Select <input type="button" value="v"/>



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.

^ Certificate Attributes






* Attribute

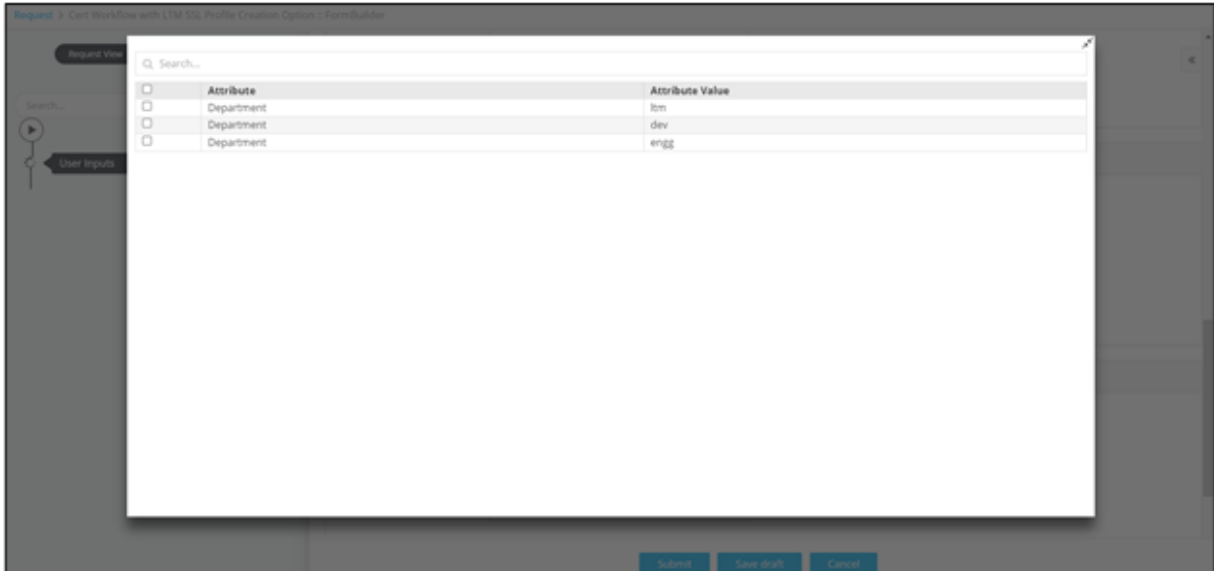
* Attribute Value

+
✎
↻
🗑

Certificate Attributes

<input type="checkbox"/>	Attribute	Attribute Value
No records found		

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.

^ Vendor Specific Details

Order Id

* Server Type

Order valid from

Order valid till

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name

- When Microsoft Enterprise is selected as CA.

^ Vendor Specific Details

* Template Name



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.

^ Notifications

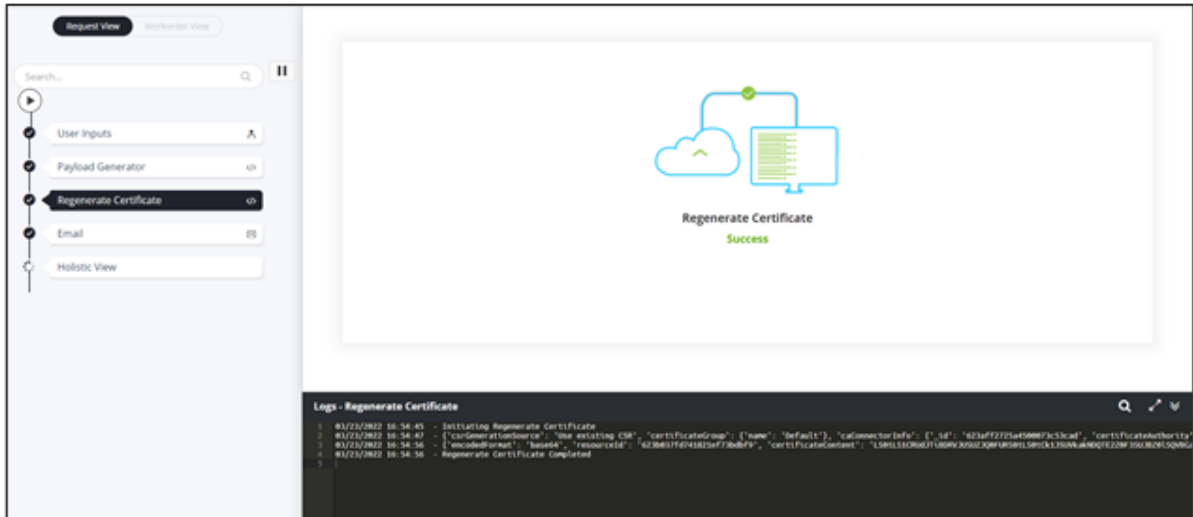
* Email ID i



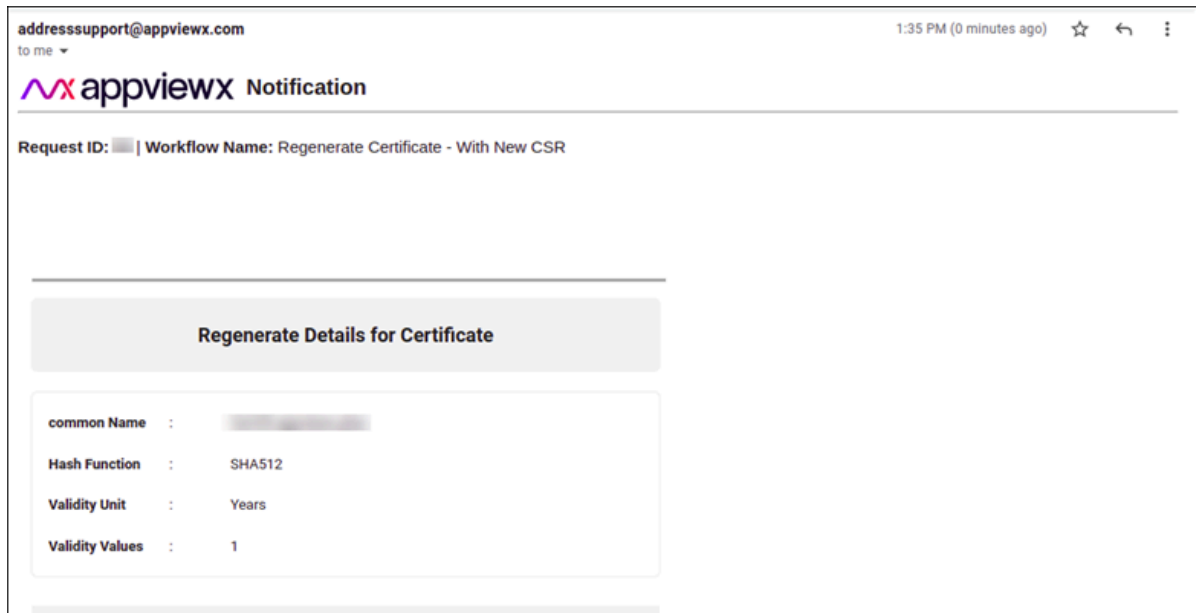
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

13. Click **Submit**.

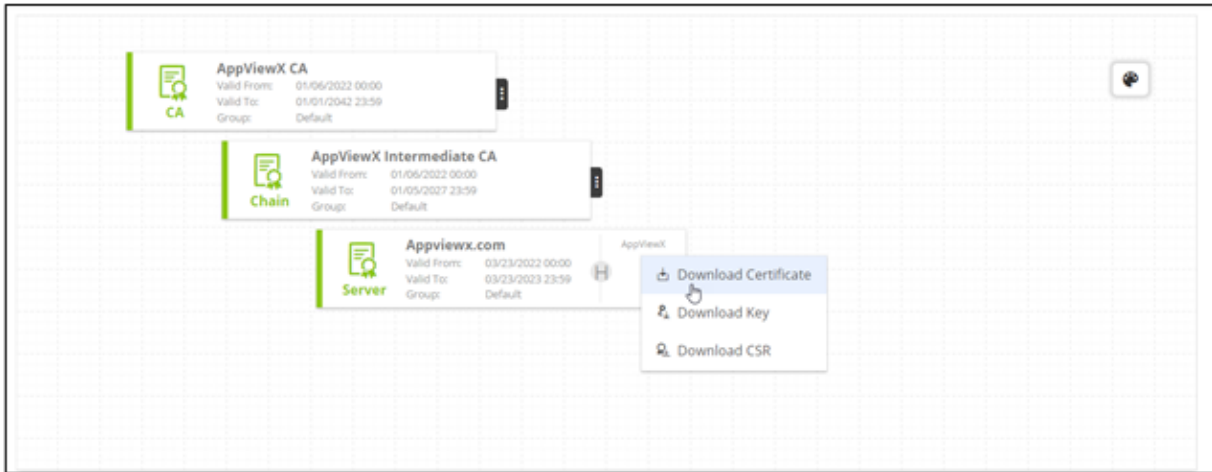
- Certificate regenerated successfully.



- 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**.

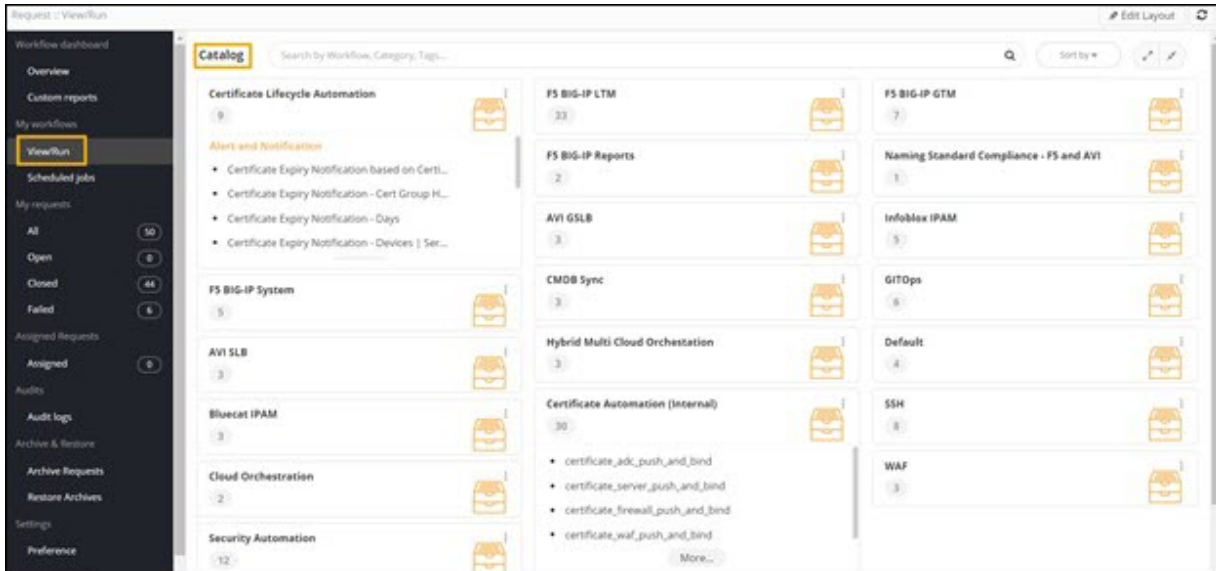




Renew Certificate and Push

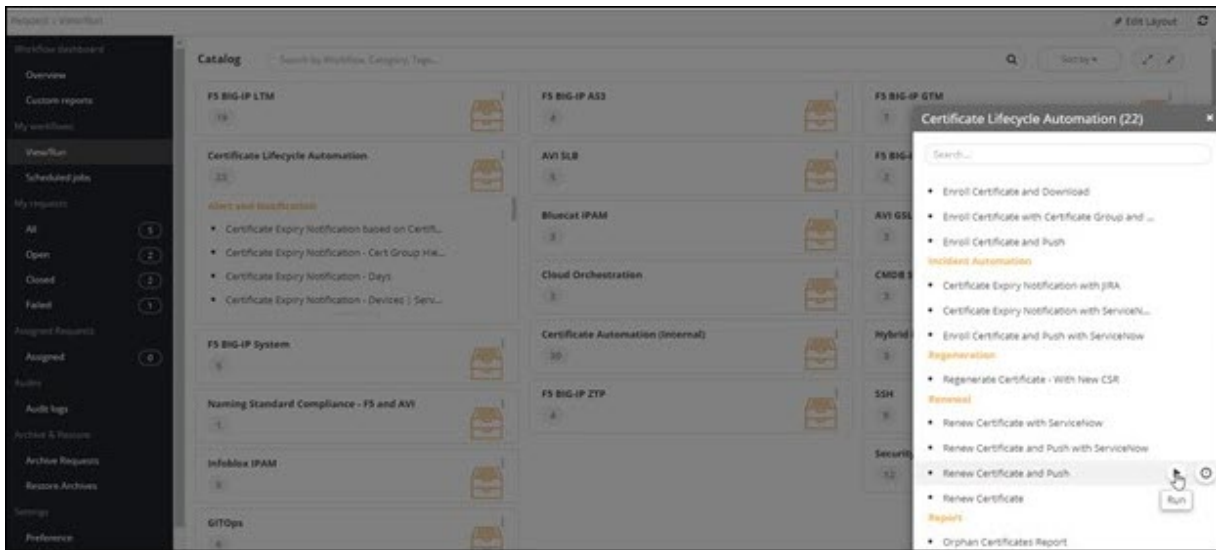
This workflow allows you to renew a certificate based on the certificate group and certificate authority and push it to the selected device.

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.


^ Certificate Information	
Certificate	Appviewx.fastneldemo E1:53:E5:72:6C:69:21:2... ▾
Serial Number	E1:53:E5:72:6C:69:21:25
CA Account	AppViewX CA


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

^ CSR Parameters	
* Common Name	Appviewx.fastneldemo
Subject Alternative Name	DNS ▾ ⓘ
DNS	Appviewx.fastneldemo ⓘ
Directory Name	
IP Address	ⓘ
Registered ID	
Other Name	
URL	
Email Address	
Organisation	
Organisation Unit	
Country	
State	

Organisation Unit	<input type="text"/>
Country	<input type="text"/>
State	<input type="text"/>
Zip Code	<input type="text"/>
* Validity Unit	Months <input type="button" value="v"/>
* Validity Value	6 <input type="button" value="v"/>
Key Type	RSA
Bit Length	2048
* Hash Function	SHA256 <input type="button" value="v"/>






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

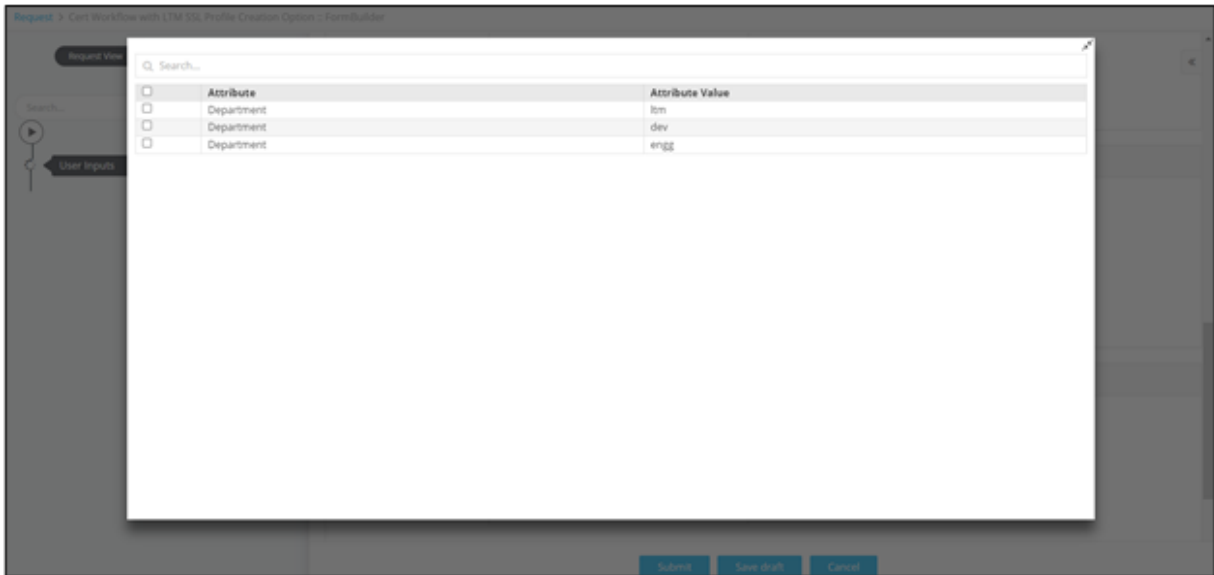
Field	Description
* Common Name	<p>Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You have the option to change the common name of the regenerated certificate. </div>
Subject Alternative Name	<p>Select the SAN as either:</p> <ul style="list-style-type: none"> • Directory Name • Email • Registered ID • URL • Other Name

Field	Description
	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>

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

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

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

Vendor Specific Details

Order Id

* Server Type

Order valid from

Order valid till

- When EJBCA is selected as CA.

^ Vendor Specific Details

* End Entity Profile Name

End entity user name

* Issuer Common Name

* Certificate Profile Name

- When Entrust is selected as CA.

^ Vendor Specific Details

Additional Emails





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.

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.

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.

Device Information

* Device Type: Server

* Vendor: LinuxServer

* Device: Linux19

* Linux Actions: Default

* Profiles/Application: LinuxServerDefault:@Linux19


* KDB Password:

+ ✎ ↺ 🗑️

* Push to Devices

Search...

<input type="checkbox"/>	Vendor	Device	Linux Actio...	Profiles/Application	KDB Passwo...
<input type="checkbox"/>	LinuxServer	Linux19	Default	LinuxServerDefault:@Li...	*****





 **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.

* Push to Devices


Q Search...

<input type="checkbox"/>	Vendor	Device	Linux Actions	Profiles/Application	Password
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****
<input type="checkbox"/>	F5	gs-f5-pe225.la...		gs-f5-pe225.lab.appvi...	*****

gs-f5-pe225.lab.appviewx.net,gs-f5-pe225.lab.appviewx.net:@KAN:@rrr,gs-f5-pe225.lab.appviewx.net:@NYC_test_vip_dont_delete_client_ssl:@Common

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.

^ Notifications

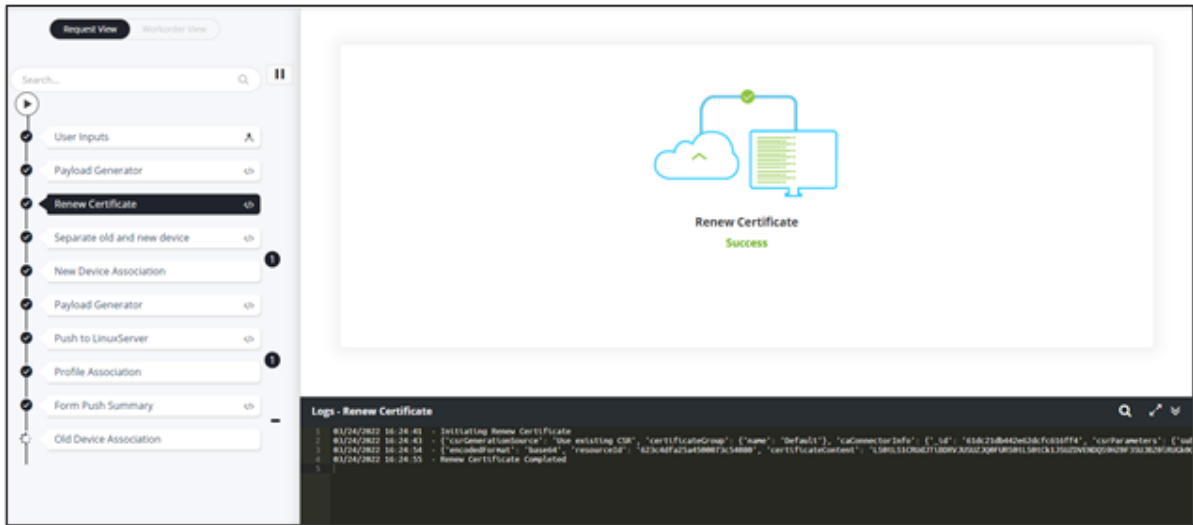
* Email ID 



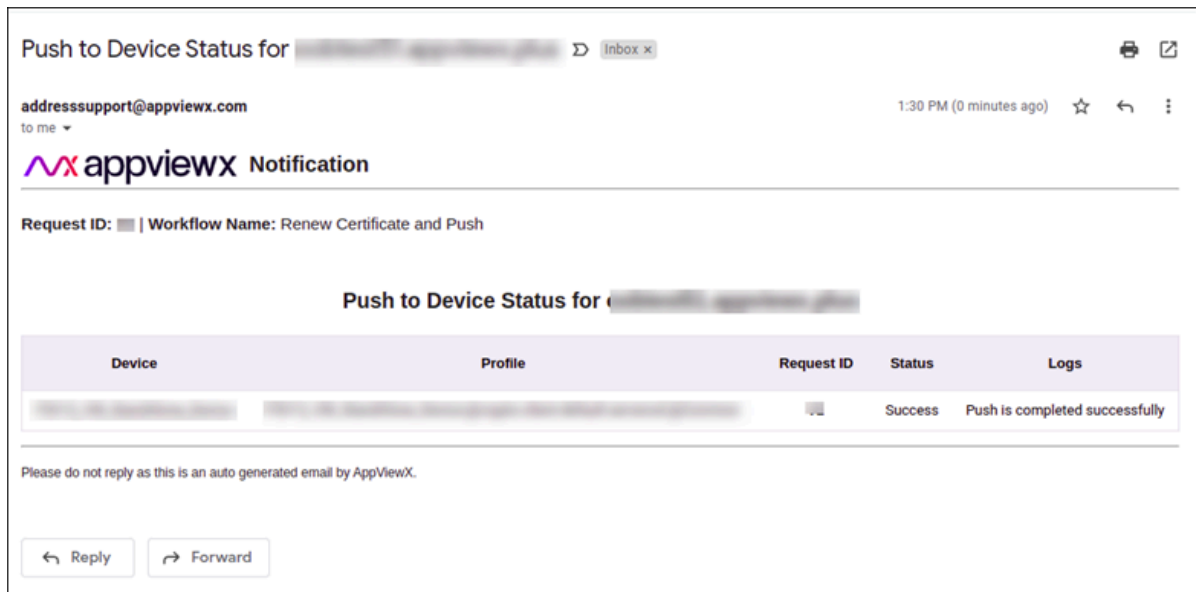
Note: The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

27. Click **Submit**.

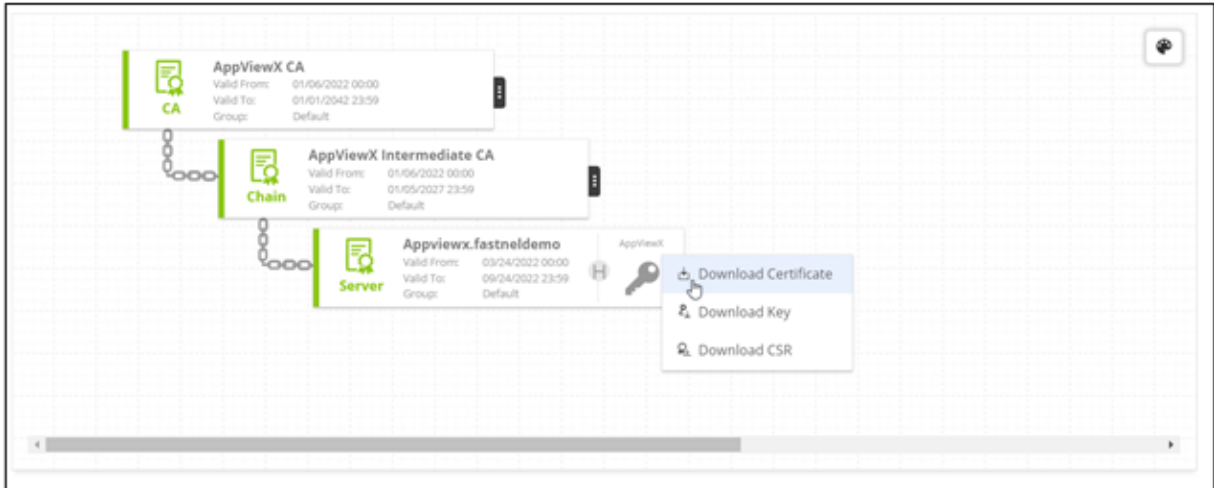
- Certificate renewed successfully.



- 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**.

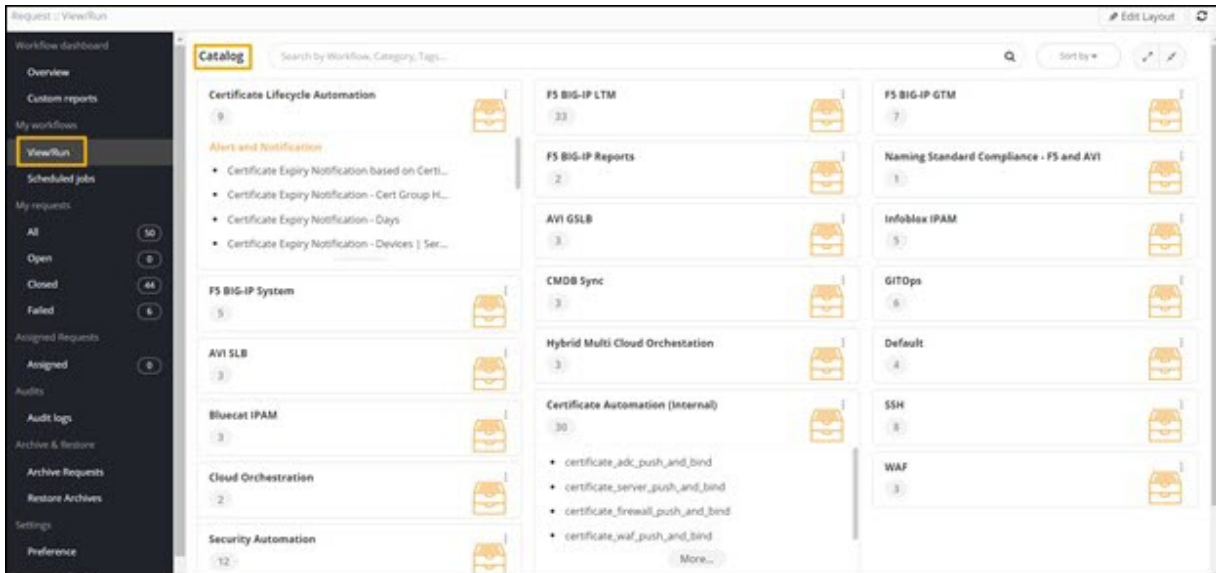




Renew Certificate with ServiceNow

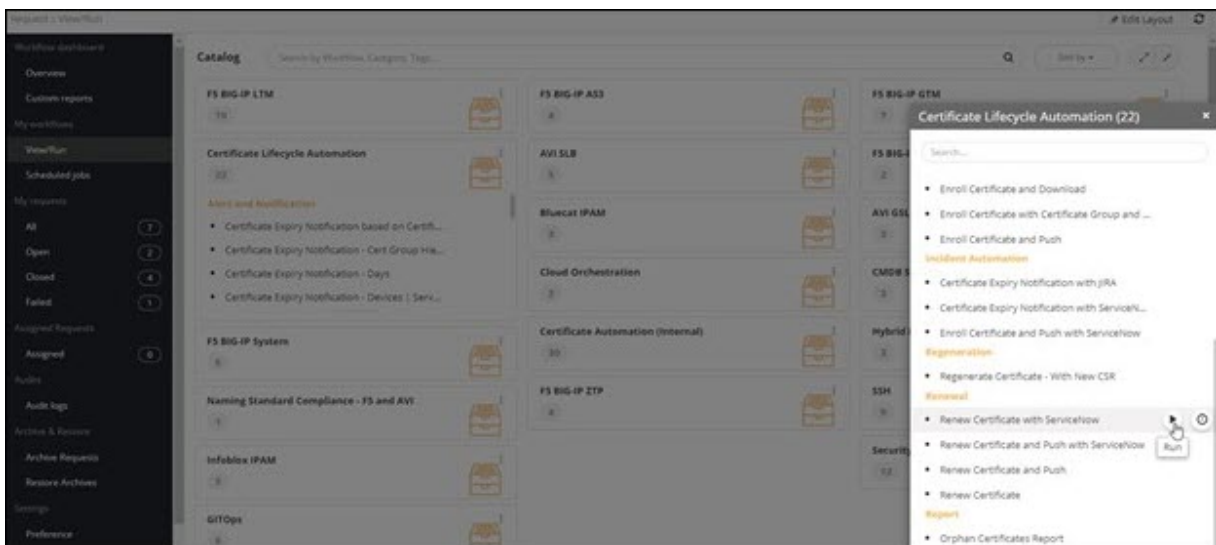
This workflow allows you to renew a certificate based on the certificate group and certificate authority and attach the renewed certificate to the ServiceNow ticket.


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.

^ Certificate Information	
* Certificate	AppViewX Inc. A4:9A:BB:56:A7:3A:EB:6F:05:06:... ▾
* Serial Number	A4:9A:BB:56:A7:3A:EB:6F:05:06:05:3F:54:A0:75:18

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






^ CSR Parameters	
* Common Name	Appviewx.com
Subject Alternative Name	Select ▾
DNS	Appviewx.com
IP Address	
Directory Name	
URL	
Other Name	
Registered ID	
Validity Unit	Years ▾
Validity Value	1 ▾
* Hash Function	SHA256 ▾
* Download Format	PEM (*.crt) ▾

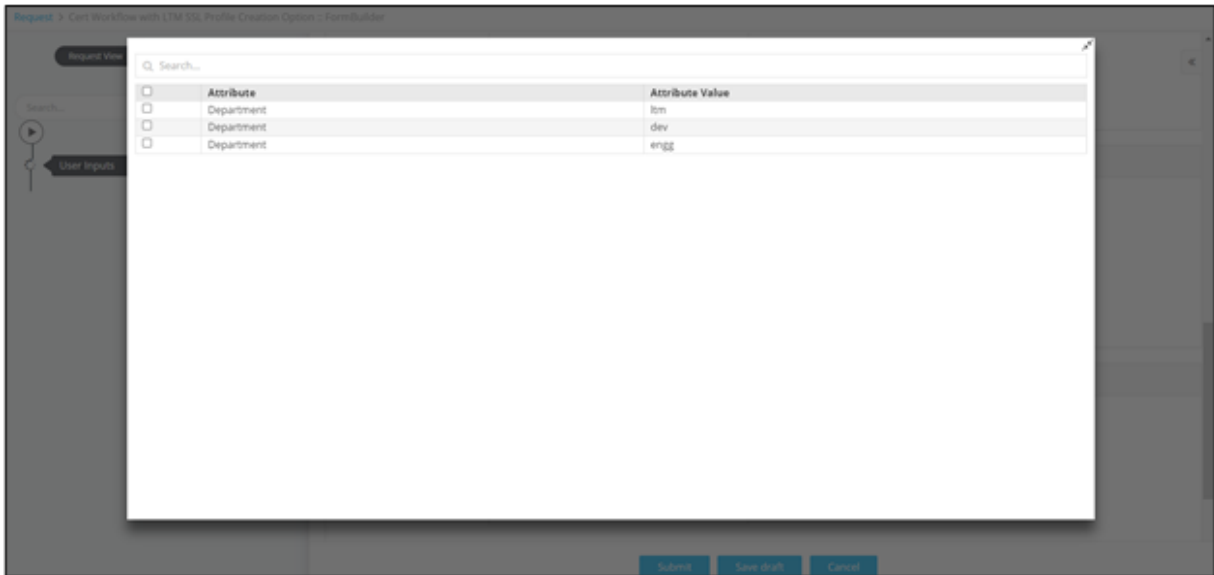
The following table describes the fields in the **CSR Parameters** section:

Field	Description
*Common Name	<p>Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You have the option to change the common name of the regenerated certificate. </div>
Subject Alternative Name	<p>Select the SAN as either:</p> <ul style="list-style-type: none"> • 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	<p>Select the Validity Unit as either:</p> <ul style="list-style-type: none"> • 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.	

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

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

ServiceNow Details



Do you require SNOW integration Yes No

RITM Ticket Number

ServiceNow Account

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.

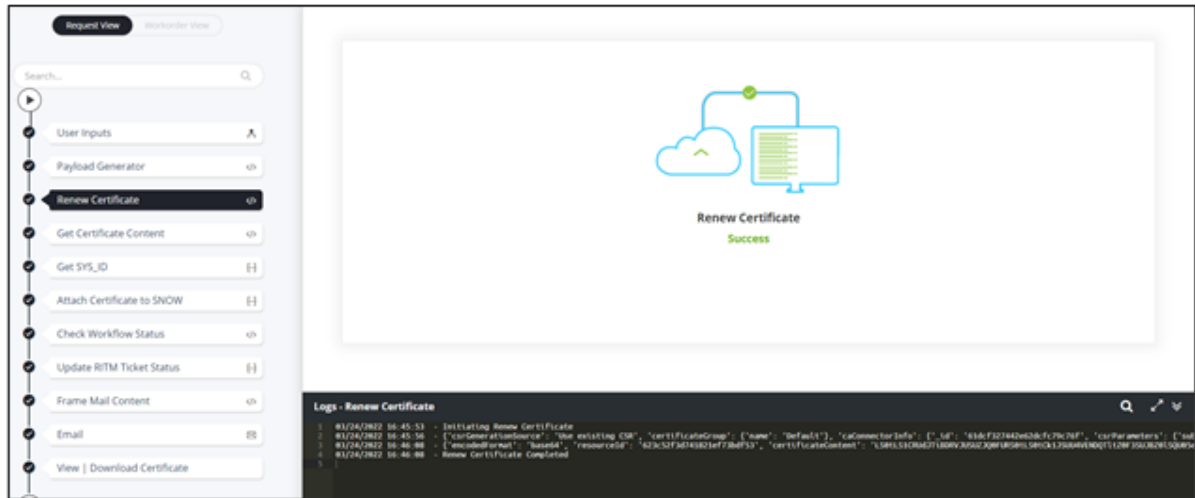
^ Notifications

* Email ID ⓘ

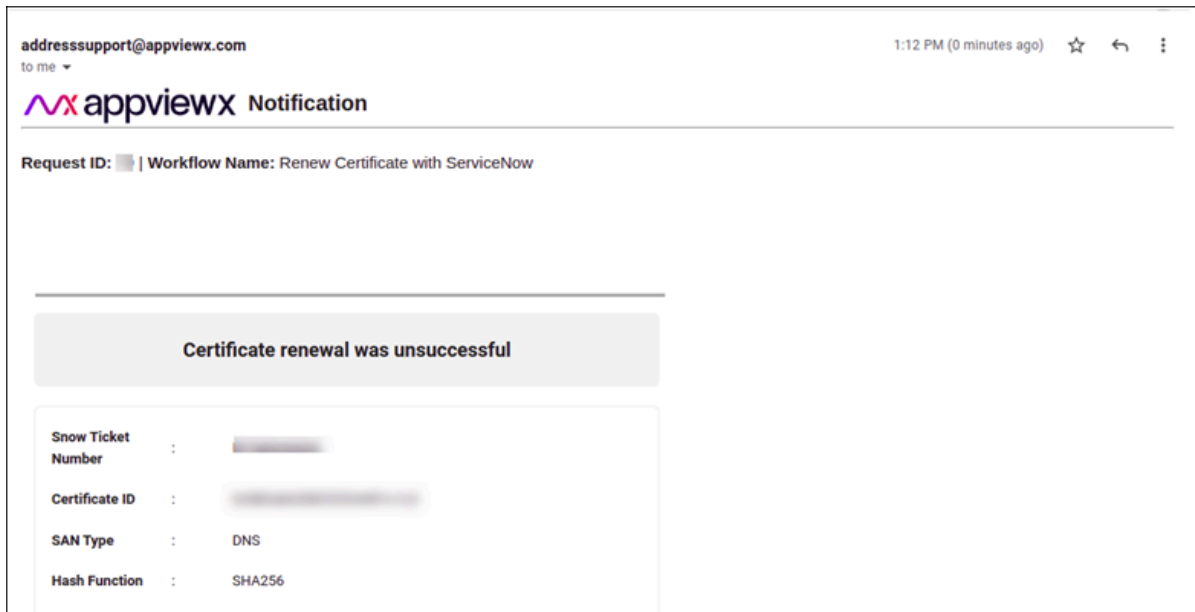
 **Note:** The **Email ID** field will auto-populate with the logged in user's email address by default if the email address has been configured in the SMTP settings. You can also enter a different email address in this field or enter multiple email addresses separated by commas.

20. Click **Submit**.

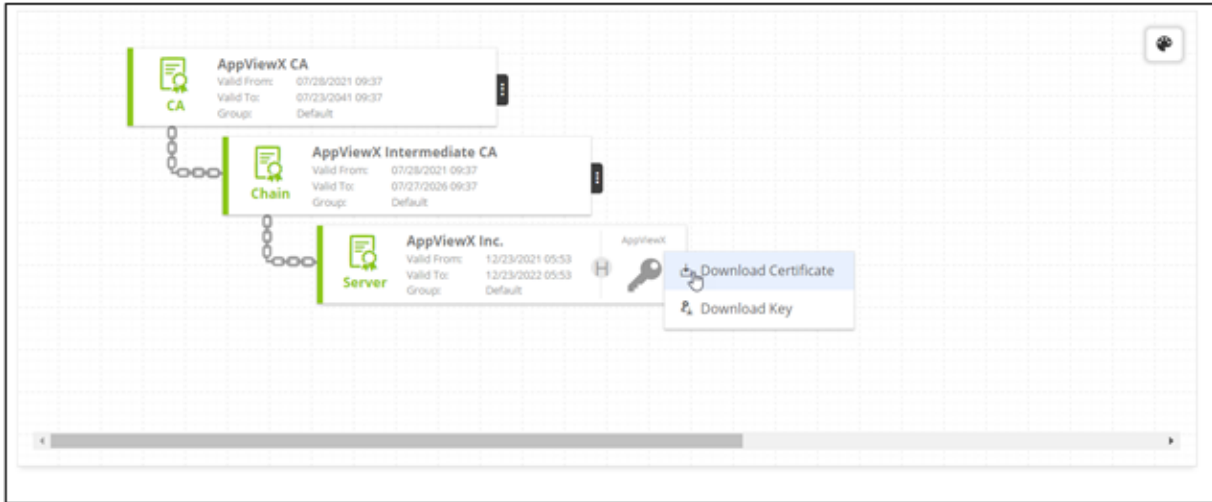
- Certificate renewed successfully.



- 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**.

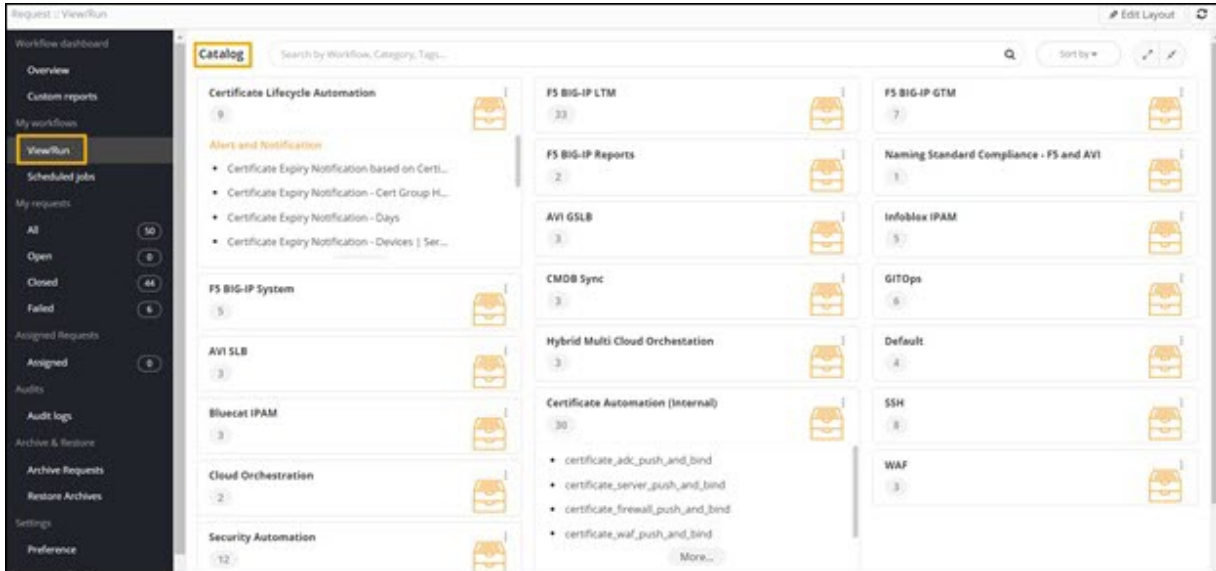




Renew Certificate and Push with ServiceNow

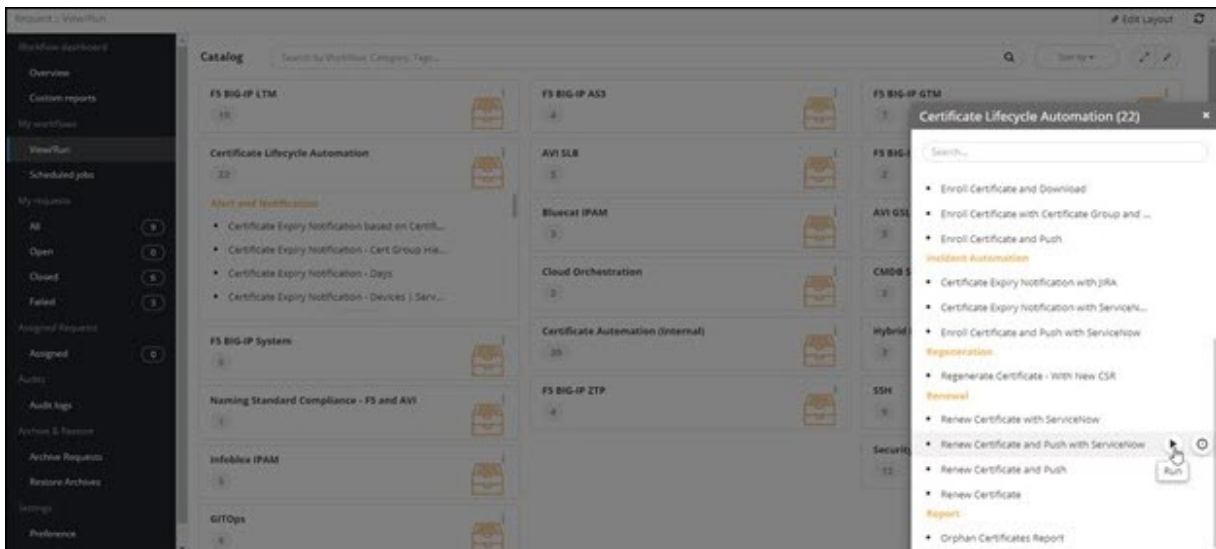
This workflow allows you to renew a certificate based on the certificate group and certificate authority, push it to a device, and attach the renewed certificate to the ServiceNow ticket.


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.

Request > Renew Certificate and Push with ServiceNow > FormBuilder

Request View

Search...

User inputs

Info

This workflow allows you to Renew a certificate corresponding to the ticket raised on ServiceNow (RTM) and push it to same old device.

1. Select the Certificate Type and Group.
2. Select the CA Details. Only the successfully configured CAs will be displayed in the drop

General Information

* Certificate Type Server Client

* Assign Group Certificate-Gateway

CA Details

* Certificate Authority Select

Certificate Information

Certificate Select

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

General Information

* Certificate Type Server Client

* Assign Group Default

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

CA Details

* Certificate Authority AppViewX


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.

^ Certificate Information	
Certificate	Appviewx.com F1:63:2A:BB:DC:EE:9D:5F:65:5A... ▾
* Serial Number	F1:63:2A:BB:DC:EE:9D:5F:65:5A:58:19:AC:9F:78:55

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






^ CSR Parameters	
* Common Name	Appviewx.com
Subject Alternative Name	DNS ▾ ⓘ
DNS	Appviewx.com ⓘ
Directory Name	
IP Address	
Registered ID	
Other Name	
URL	
Email	
* Validity Unit	Months ▾
* Validity Value	6 ▾
Hash Function	SHA256 ▾
* Download Format	PEM (*.crt) ▾

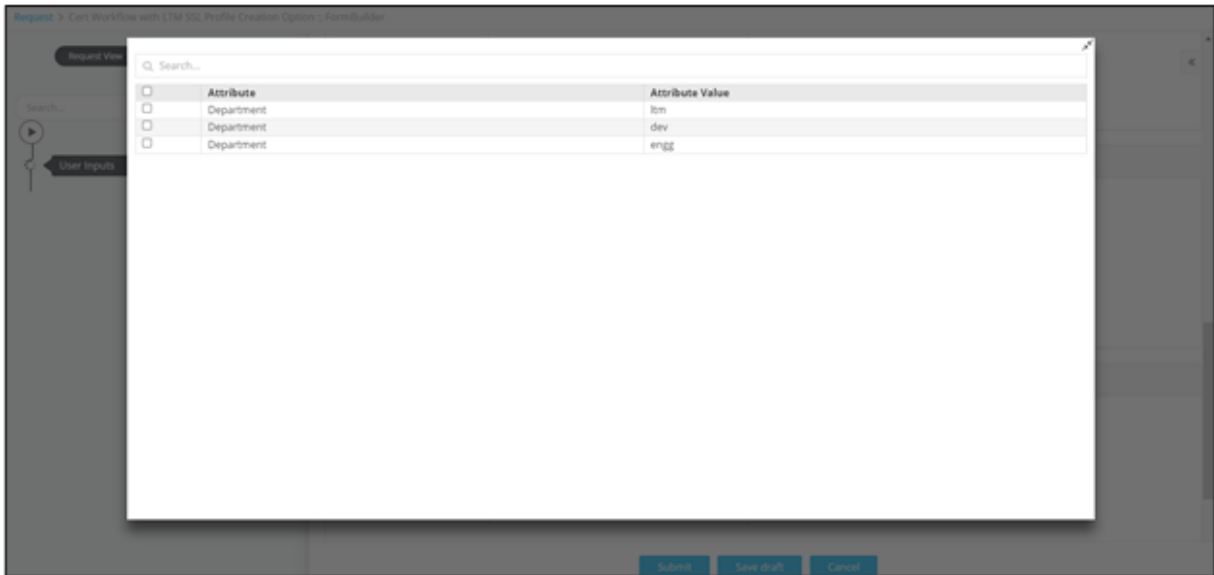
The following table describes the fields in the **CSR Parameters** section:

Field	Description
*Common Name	<p>Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: You have the option to change the common name of the regenerated certificate. </div>
Subject Alternative Name	<p>Select the SAN as either:</p> <ul style="list-style-type: none"> • 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	<p>Select the Validity Unit as either:</p> <ul style="list-style-type: none"> • 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.

ServiceNow Details



Do you require SNOW integration Yes No

RITM Ticket Number

ServiceNow Account

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.

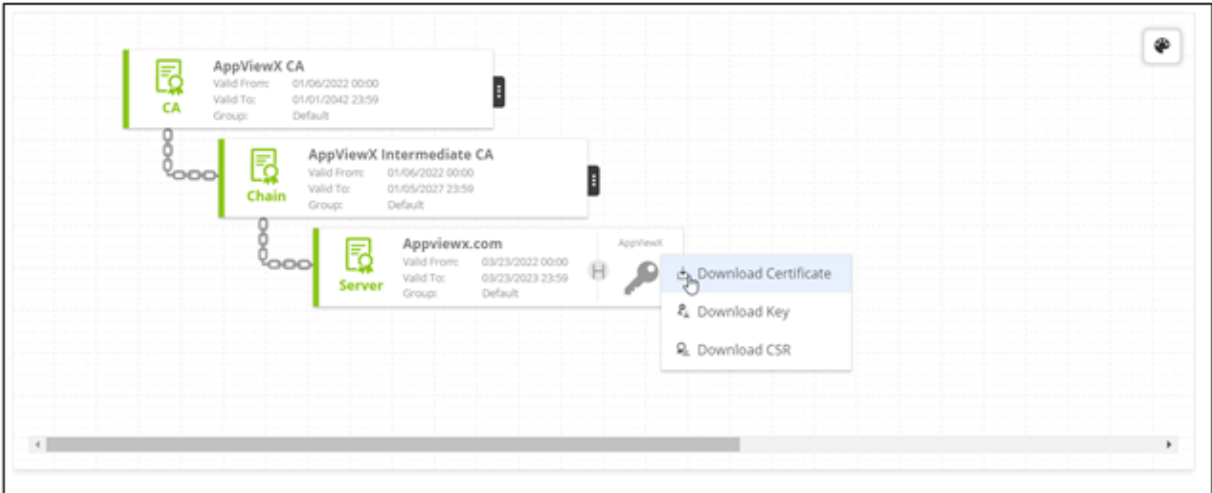
19. Under the **Notifications** section, enter the **Email ID** to which the certificate creation notification will be sent.

^ Notifications

* Email ID

 **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**.



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



Chapter 8: Automation Workflow Tasks

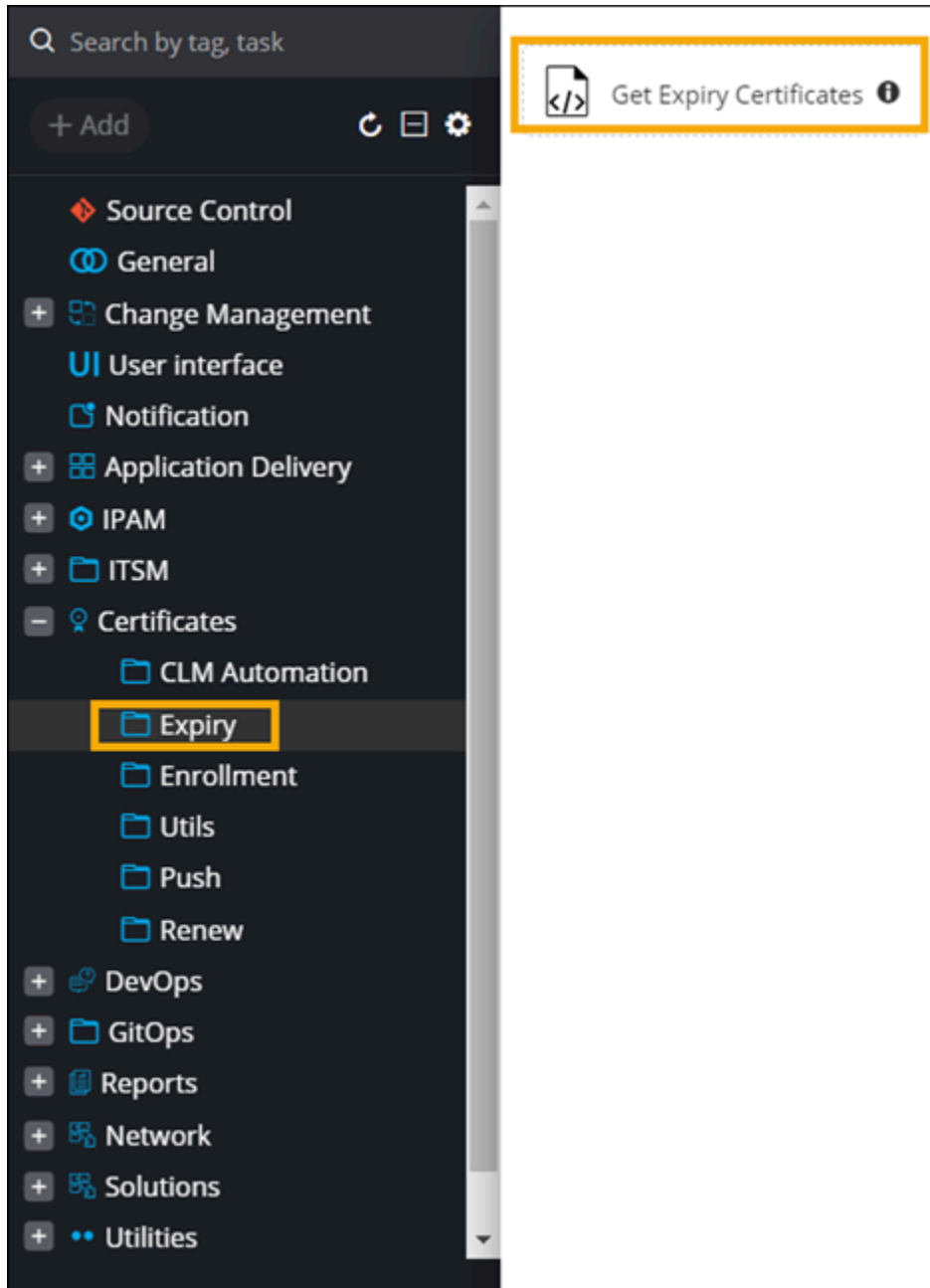
- [Overview](#)
- [Expiry Task](#)
- [Enrollment Tasks](#)
- [Renew Tasks](#)
- [Push Tasks](#)

Overview

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

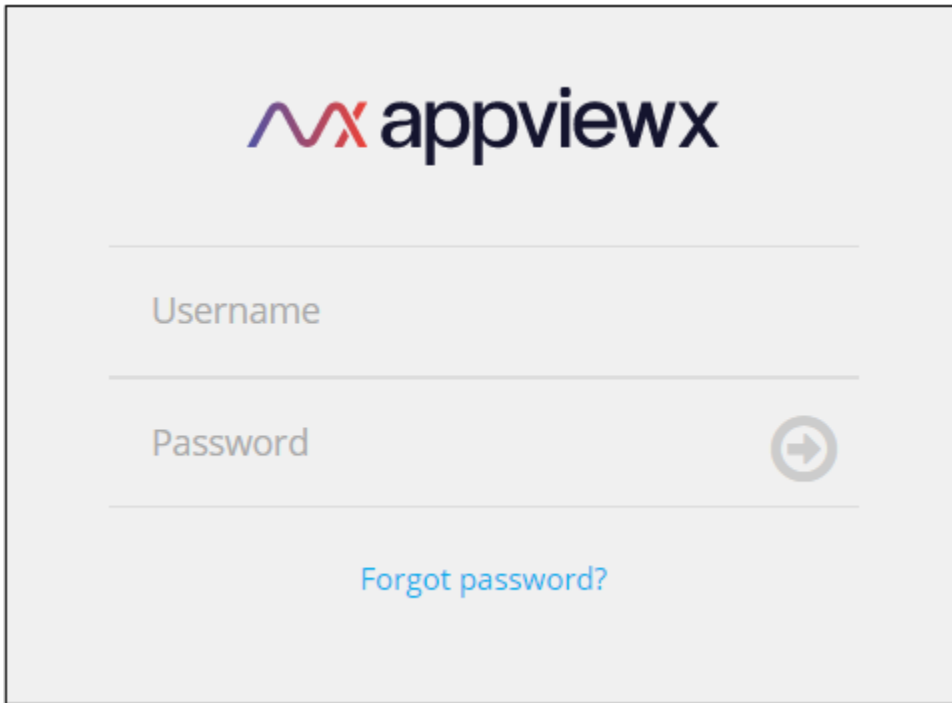
Expiry Task


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.

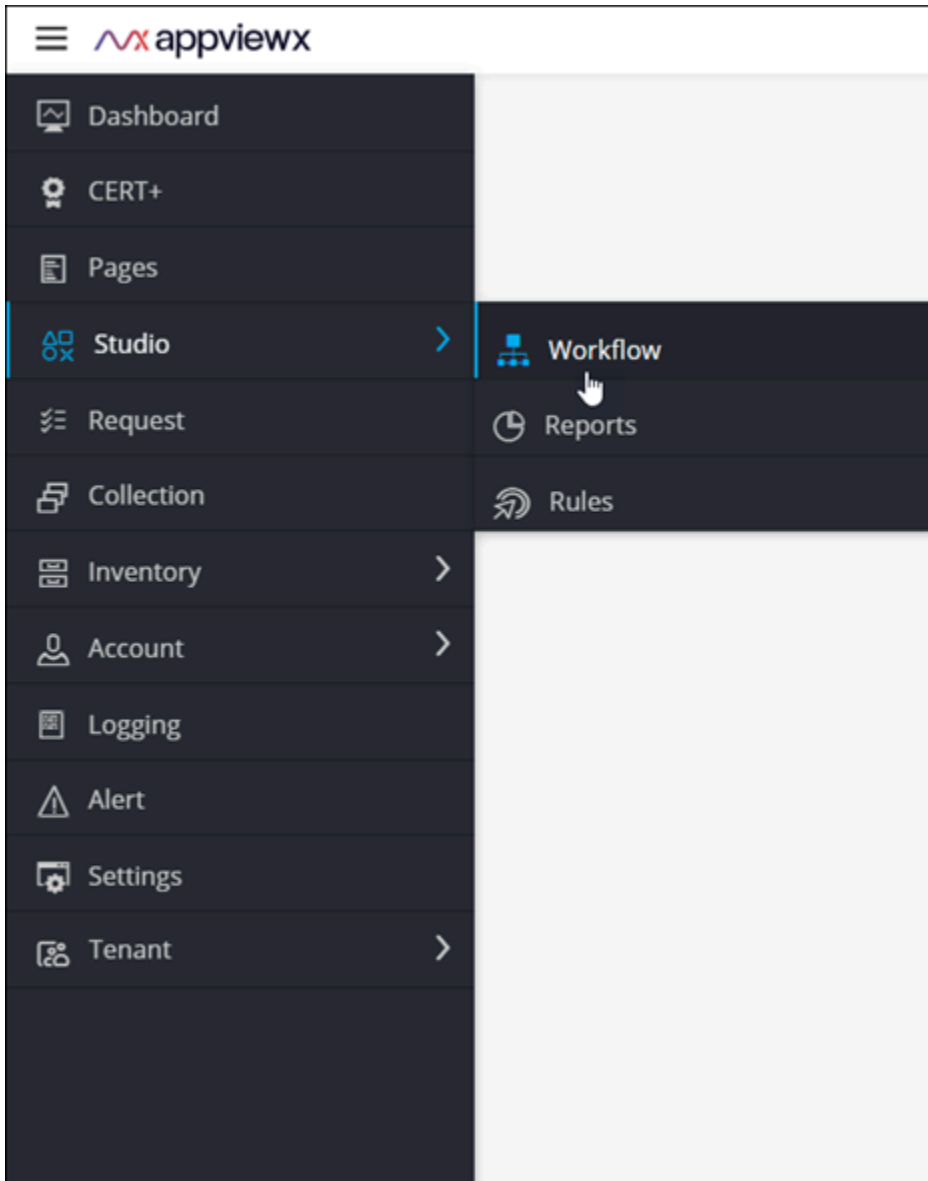


To design a custom workflow using the **Get Expiry Certificates** task

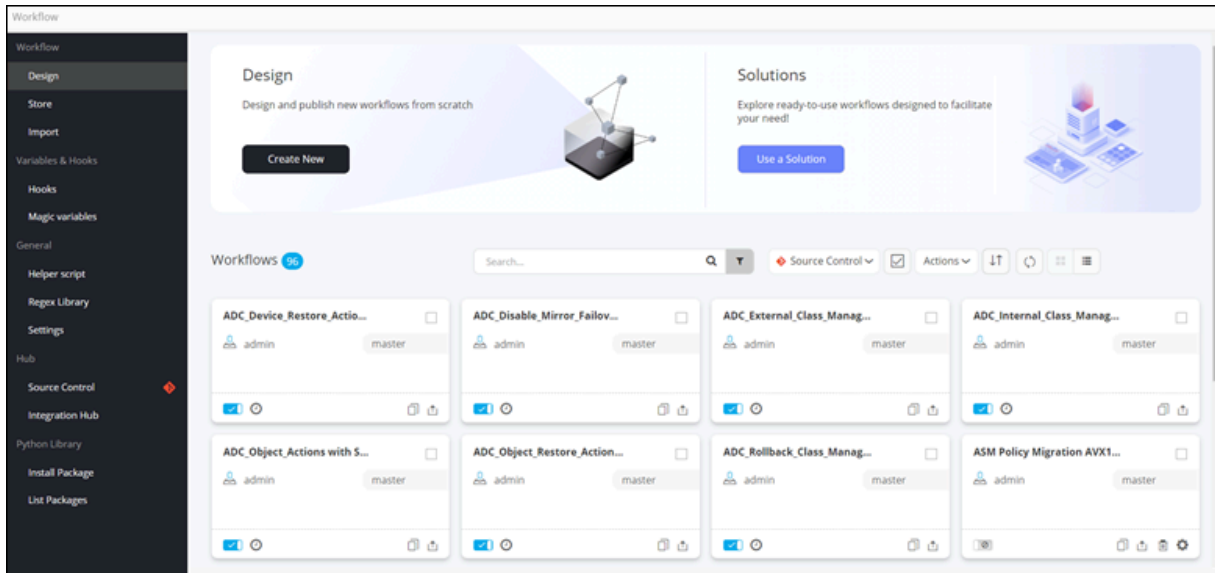
1. Log into AppViewX with valid credentials.



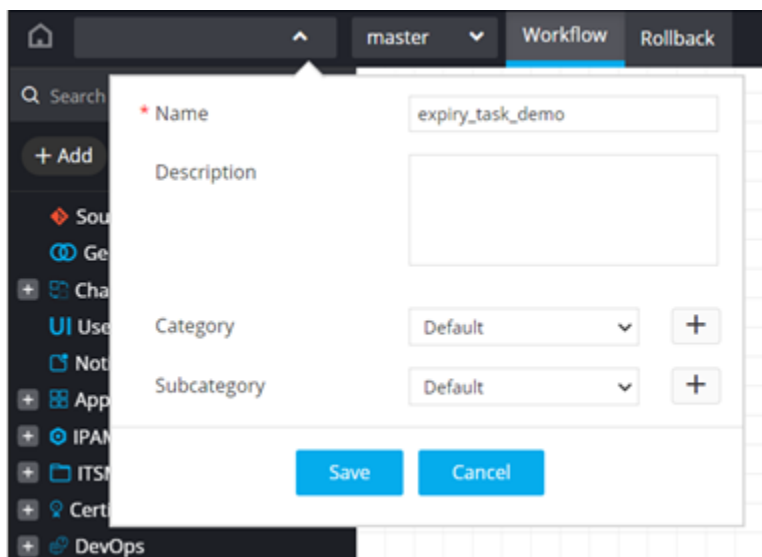
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



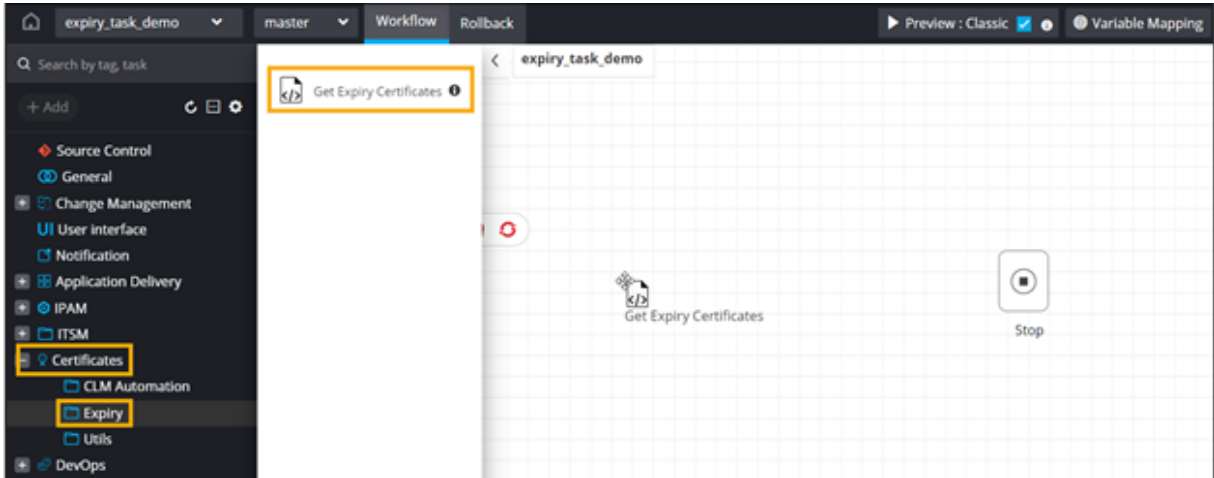
The **Workflow** inventory page is displayed.



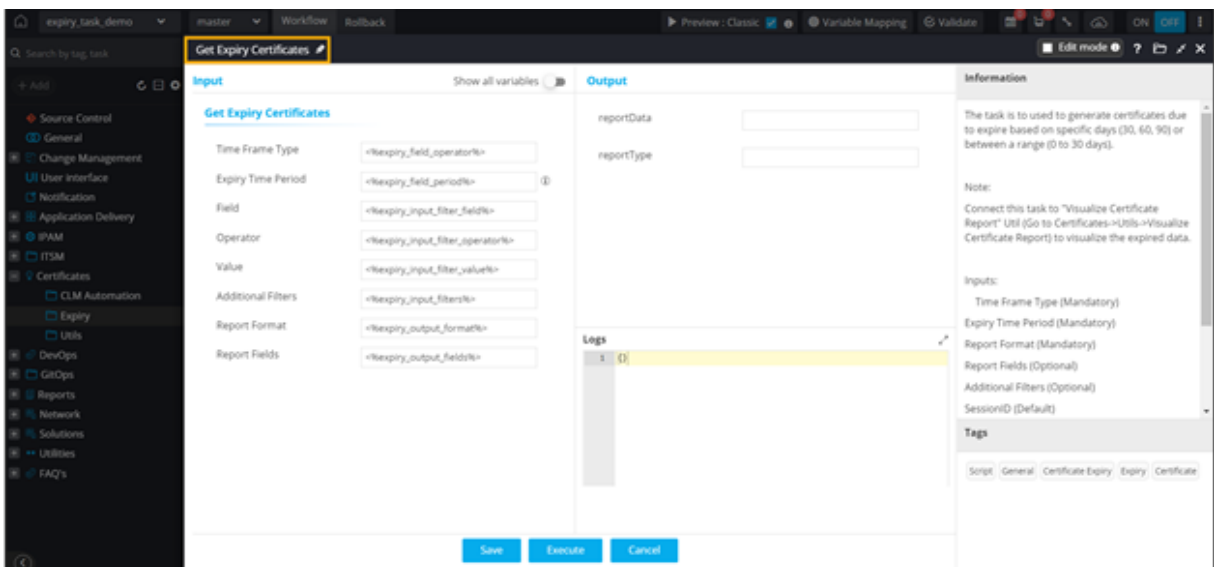
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



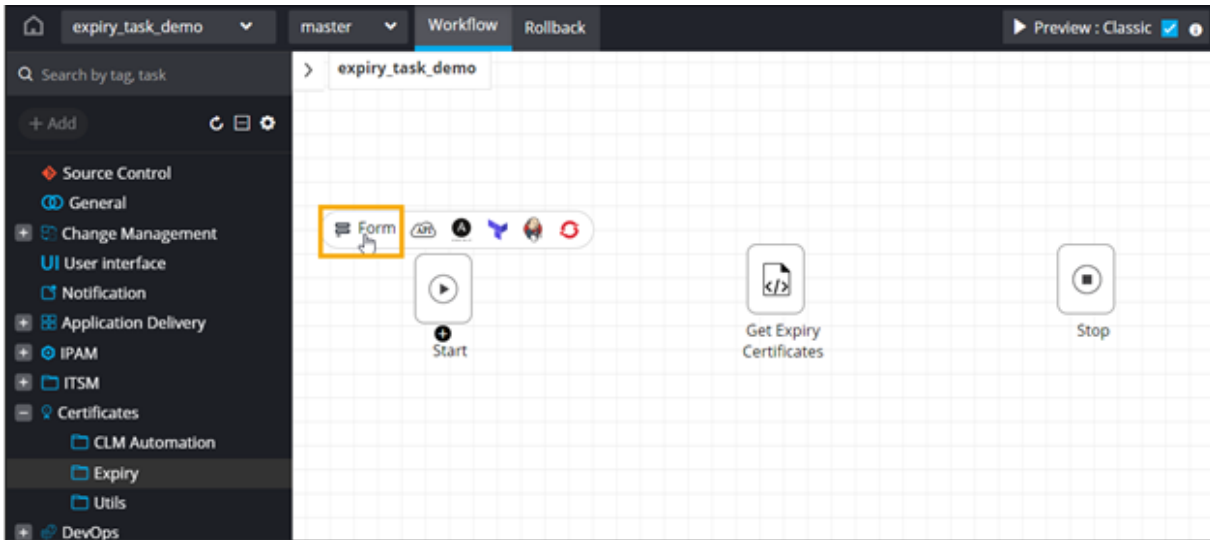
7. From the **Certificates** folder, under **Expiry**, drag and drop the **Get Expiry Certificates** task.



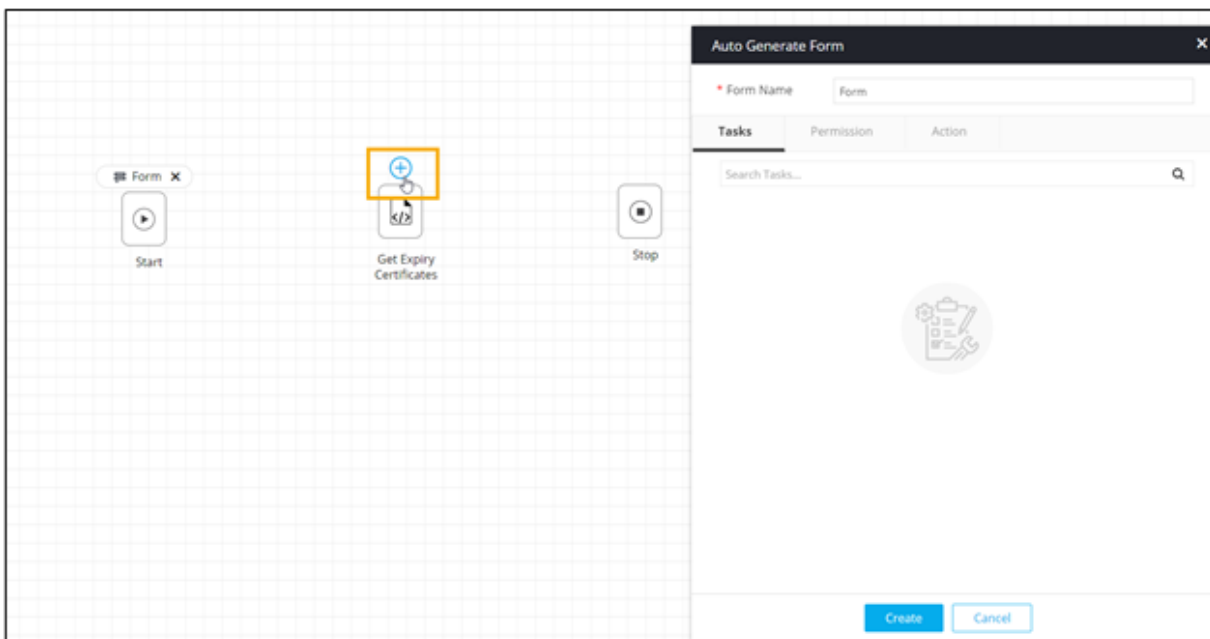
This task can be used to generate a report listing certificates due to expire in a specific number of days.



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

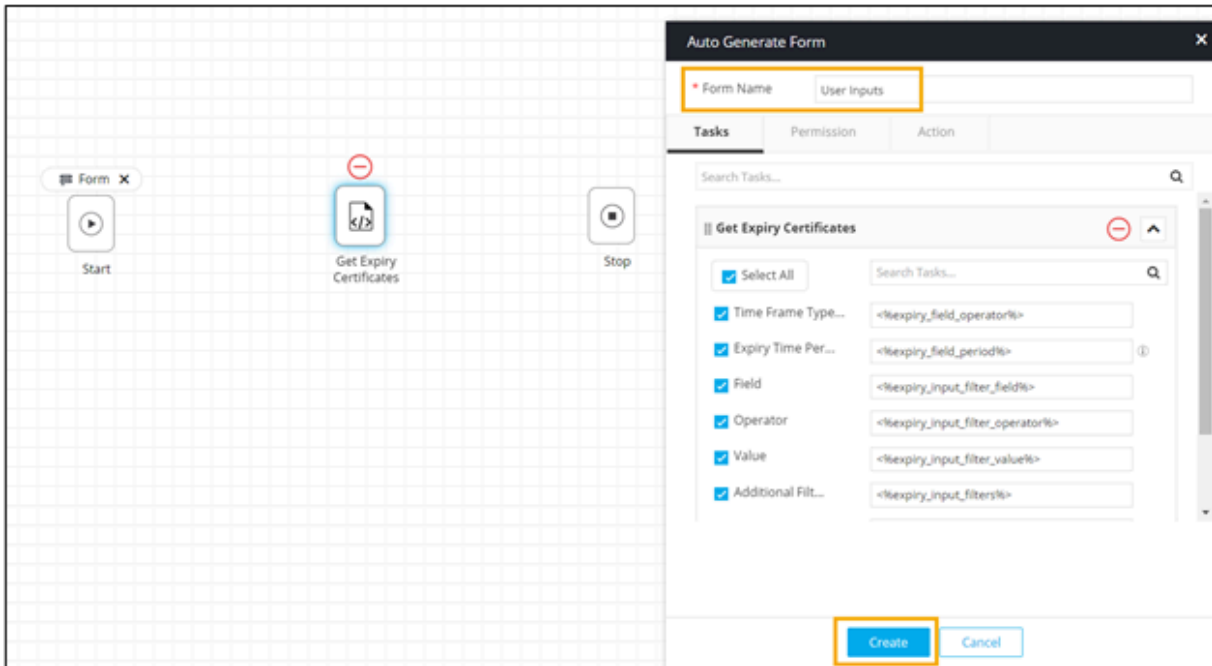


9. Click  above the **Get Expiry Certificates** task to auto-populate the form fields.

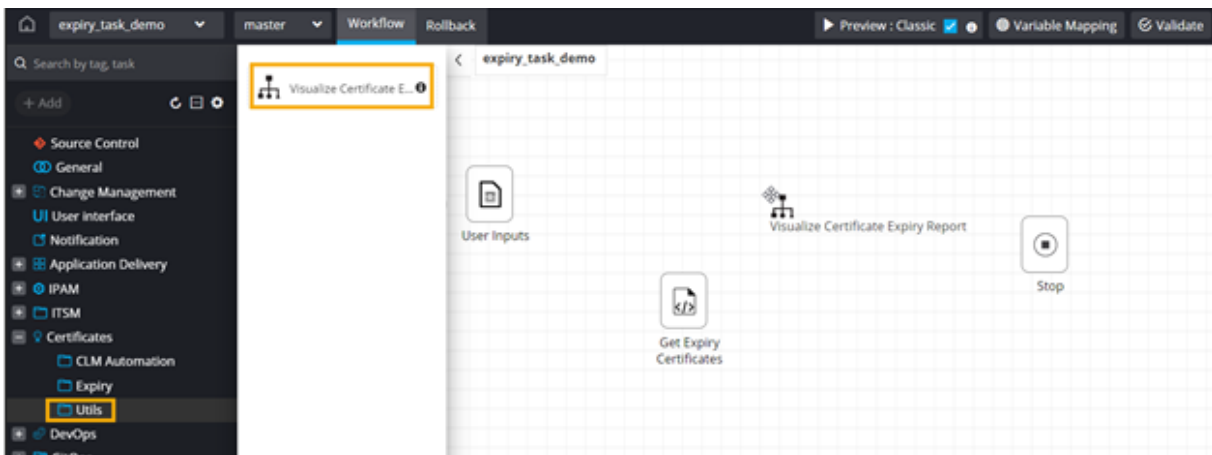


10. Select the fields required in the input form.

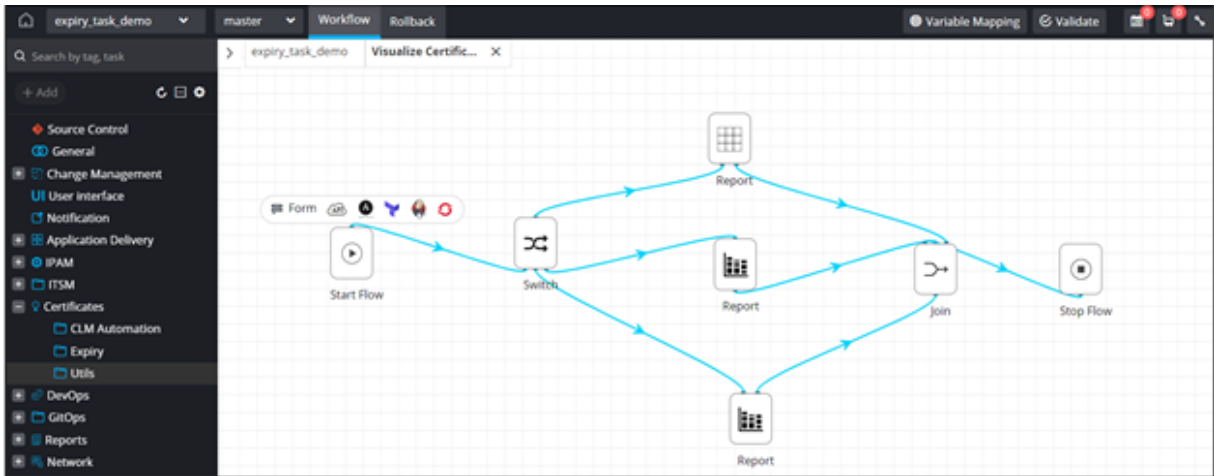
11. Provide a **Form Name** and click **Create**.



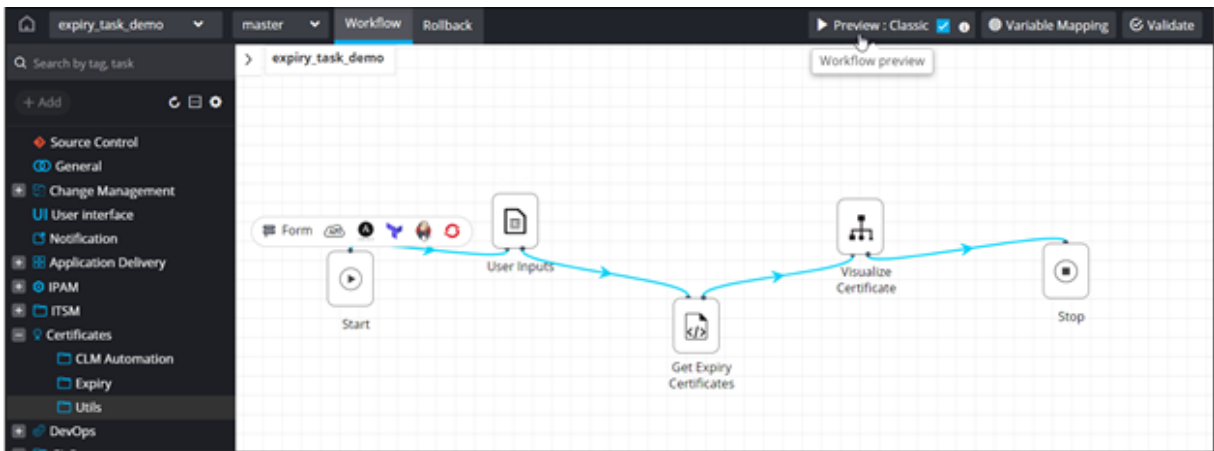
12. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.



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 screenshot shows a configuration interface for a workflow task named 'Get Expiry Certificates'. On the left, there is a sidebar with 'Request View' and 'Workorder View' tabs, a search bar, and a 'User Inputs' section. The main area contains the following fields:






- Time Frame Type:** A dropdown menu with 'Exact' selected.
- Expiry Time Period:** An empty text input field.
- Field:** A dropdown menu with 'Type' selected.
- Operator:** A dropdown menu with 'Is' selected.
- Value:** An empty text input field.

Below these fields are four action buttons: a plus sign (+), an edit icon, a refresh icon (C), and a delete icon. Further down is an 'Additional Filters' section with a search bar and a table with columns 'Field', 'Operator', and 'Value'. The table currently shows 'No records found'. At the bottom of the form are three buttons: 'Next', 'Save draft', and 'Cancel'.

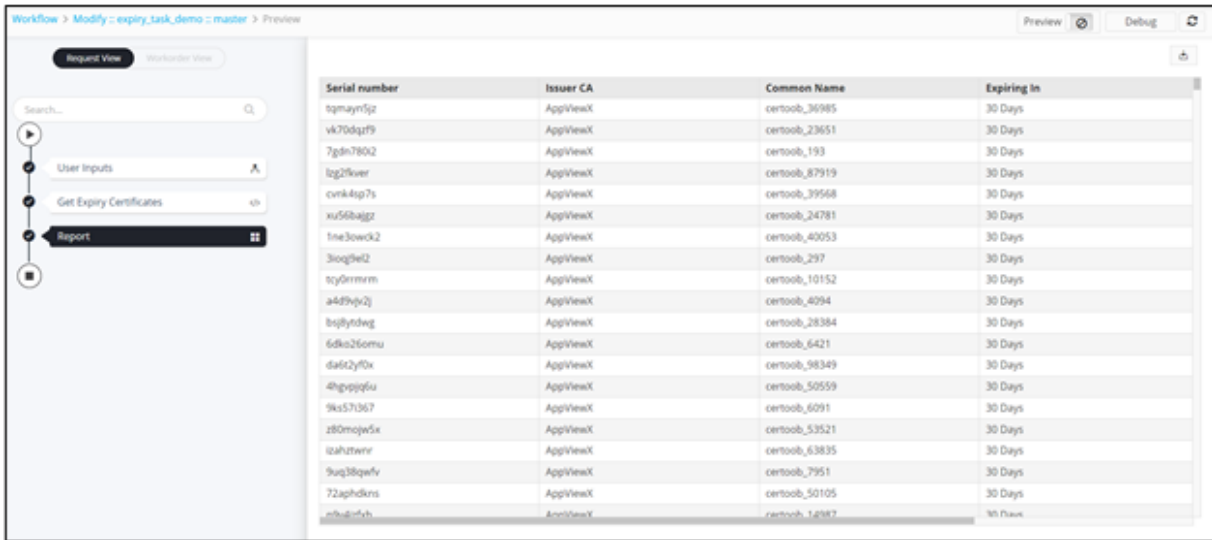
The following table describes the field information in the **User Inputs** form:

Field	Description
Time Frame Type	<p>Enter the time frame type from the available options:</p> <ul style="list-style-type: none"> • 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). <p> Note: Exact is the default selection.</p>
Expiry Time Period	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>Select the conditional operator:</p> <ul style="list-style-type: none"> • Is • Is Not

Field	Description
Value	Enter a valid value for filtering the certificates.
Additional Filters	<p>This grid displays the values selected in these fields:</p> <ul style="list-style-type: none"> • Field • Operator • Value <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: The steps to apply these additional filters are given below the table. </div>
Report Format	<p>Select the format in which the report is displayed from the available options:</p> <ul style="list-style-type: none"> • 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.



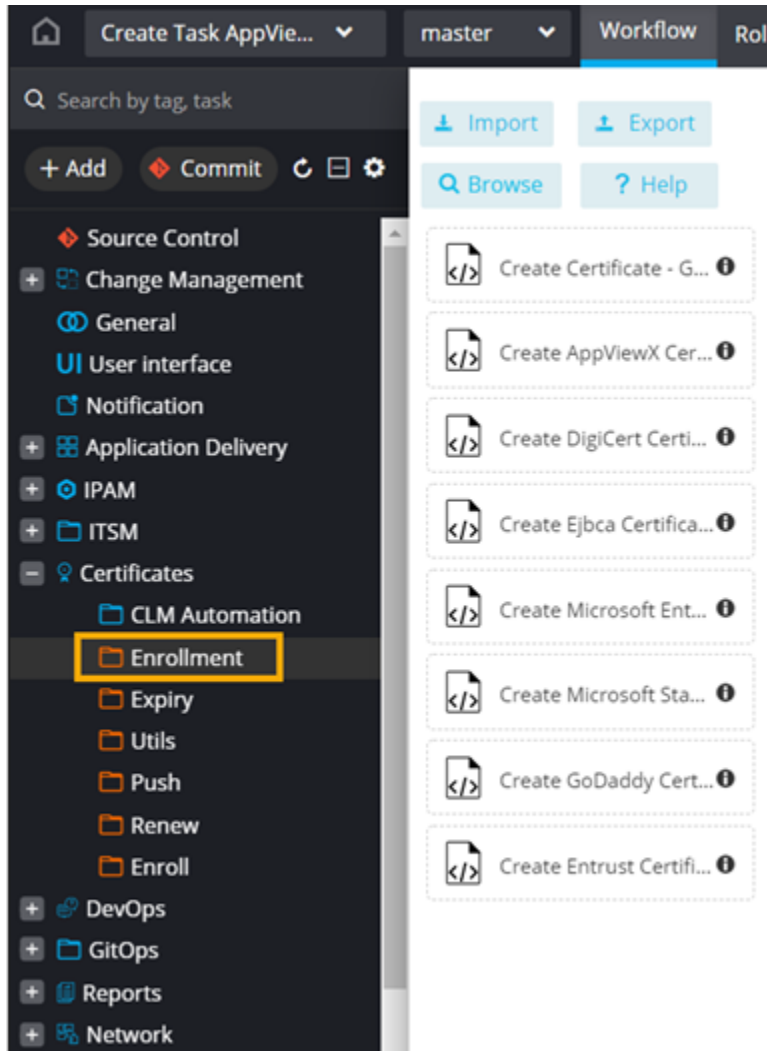
Serial number	Issuer CA	Common Name	Expiring In
tgmayn1jz	AppViewX	certoob_36985	30 Days
vk70dqzF9	AppViewX	certoob_23651	30 Days
7gdn7802	AppViewX	certoob_193	30 Days
lg2lfker	AppViewX	certoob_87919	30 Days
cvnk4sp7s	AppViewX	certoob_39568	30 Days
xu56baggt	AppViewX	certoob_24781	30 Days
1ne3owck2	AppViewX	certoob_40053	30 Days
3ioq9he2	AppViewX	certoob_297	30 Days
tcy0mrm	AppViewX	certoob_10152	30 Days
a489yv2j	AppViewX	certoob_4094	30 Days
8qjlyfweg	AppViewX	certoob_28384	30 Days
6dks26emu	AppViewX	certoob_6421	30 Days
da6t2yfox	AppViewX	certoob_98349	30 Days
4hgypqfku	AppViewX	certoob_50559	30 Days
9ks57367	AppViewX	certoob_6091	30 Days
z80mojw5x	AppViewX	certoob_53521	30 Days
iqahzwmr	AppViewX	certoob_63835	30 Days
9uq38qefv	AppViewX	certoob_7951	30 Days
72aphdkrs	AppViewX	certoob_50105	30 Days
enb4bnfch	AppViewX	certoob_14987	30 Days



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

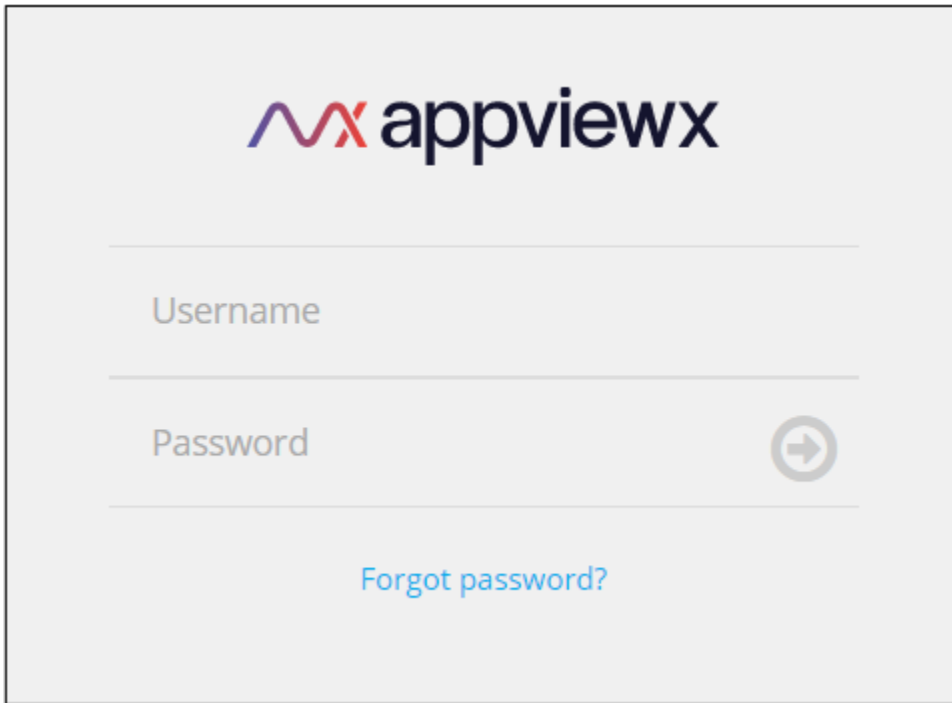
Enrollment Tasks


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.

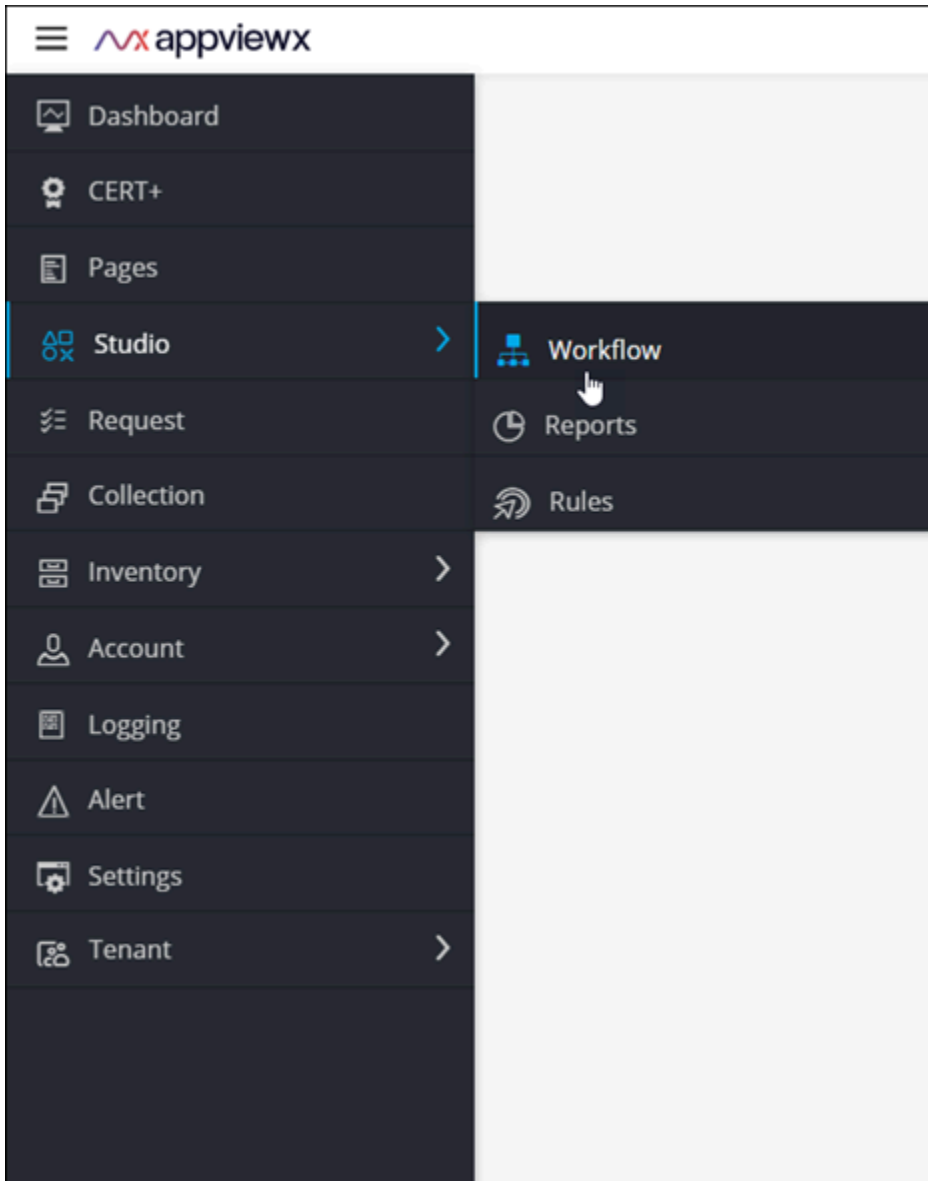


To design a custom workflow using **Enrollment** tasks:

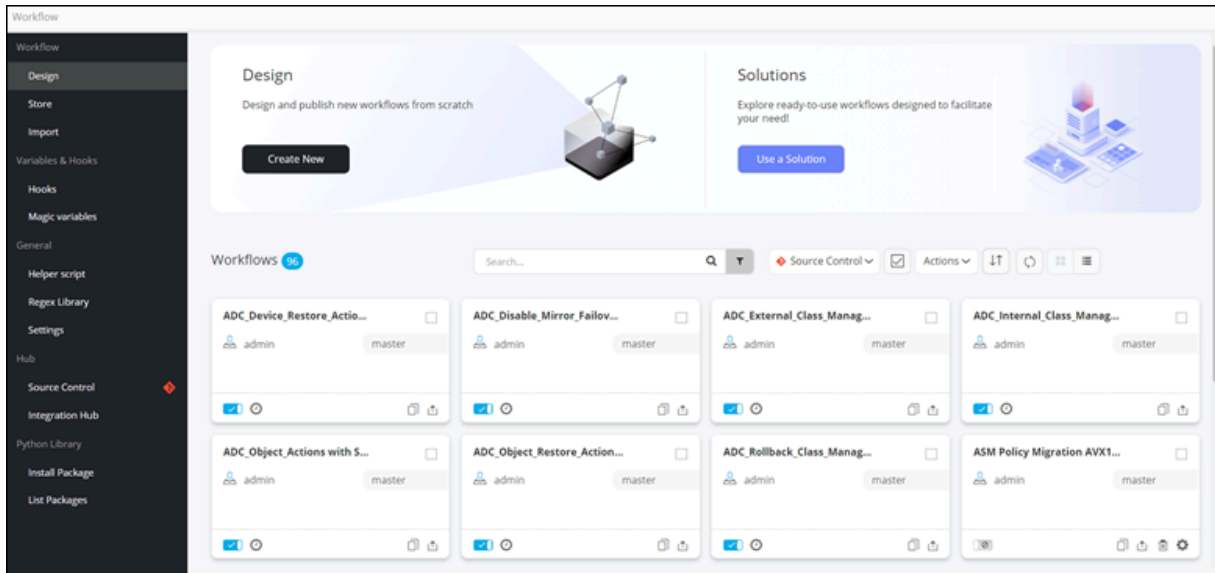
1. Log into AppViewX with valid credentials.



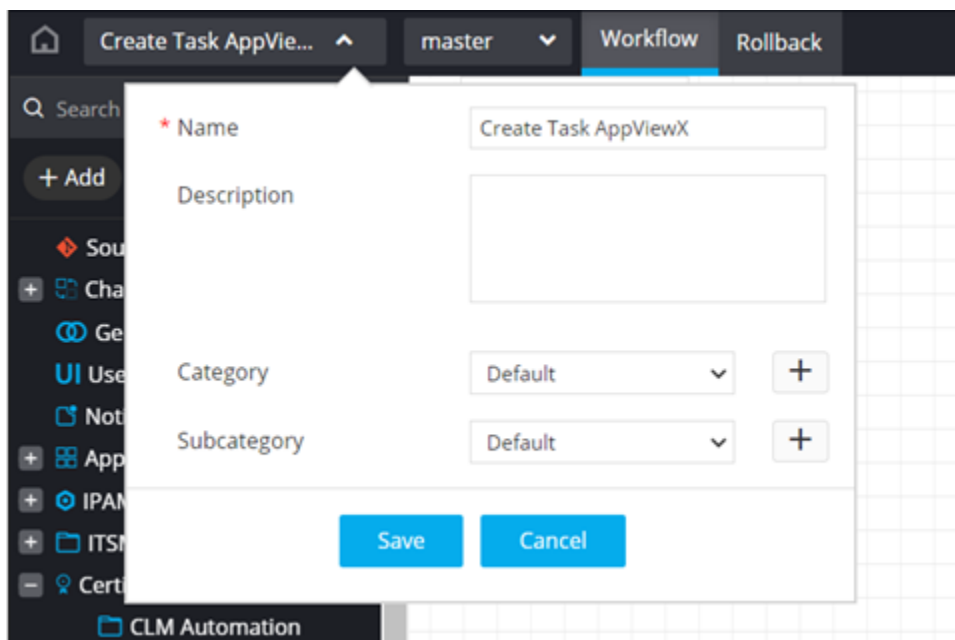
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



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**.

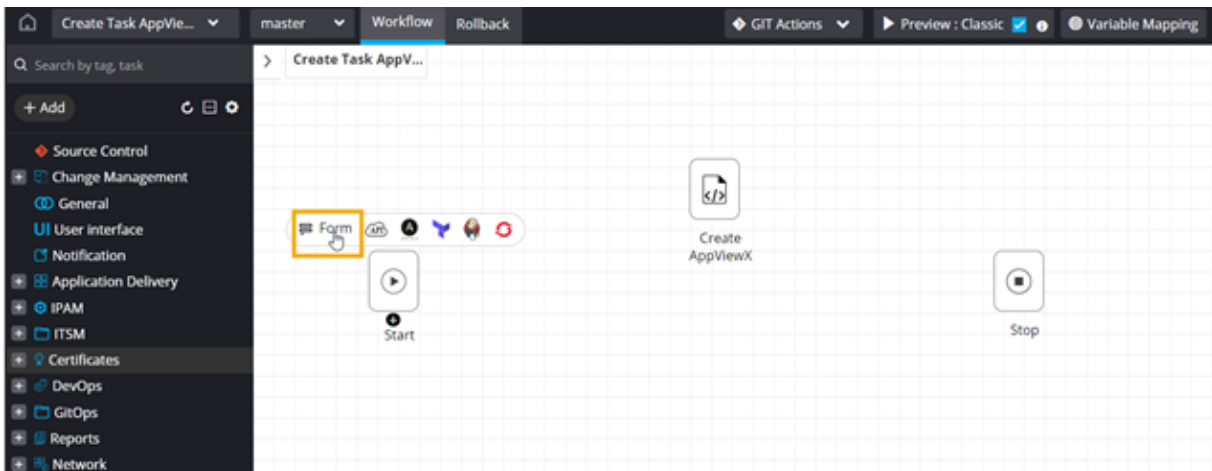


7. From the **Certificates** folder, click **Enrollment**.
The tasks for the following CAs are available in the **Enrollment** folder:
 - Appviewx
 - Digicert
 - Ejbca

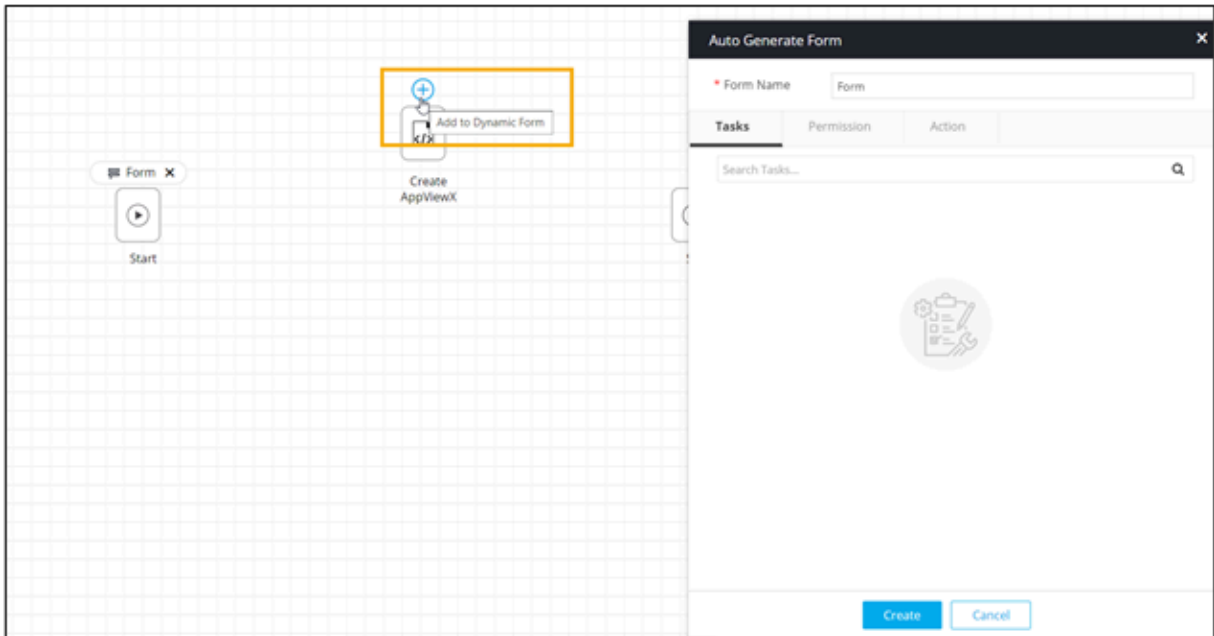
- Entrust
 - Microsoft Enterprise
 - Microsoft Standalone
 - GoDaddy
8. From the **Enrollment** folder, drag and drop any of the Create Certificate tasks. For example, the **Create AppViewX Certificate** task.

9. Click **Save**.

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

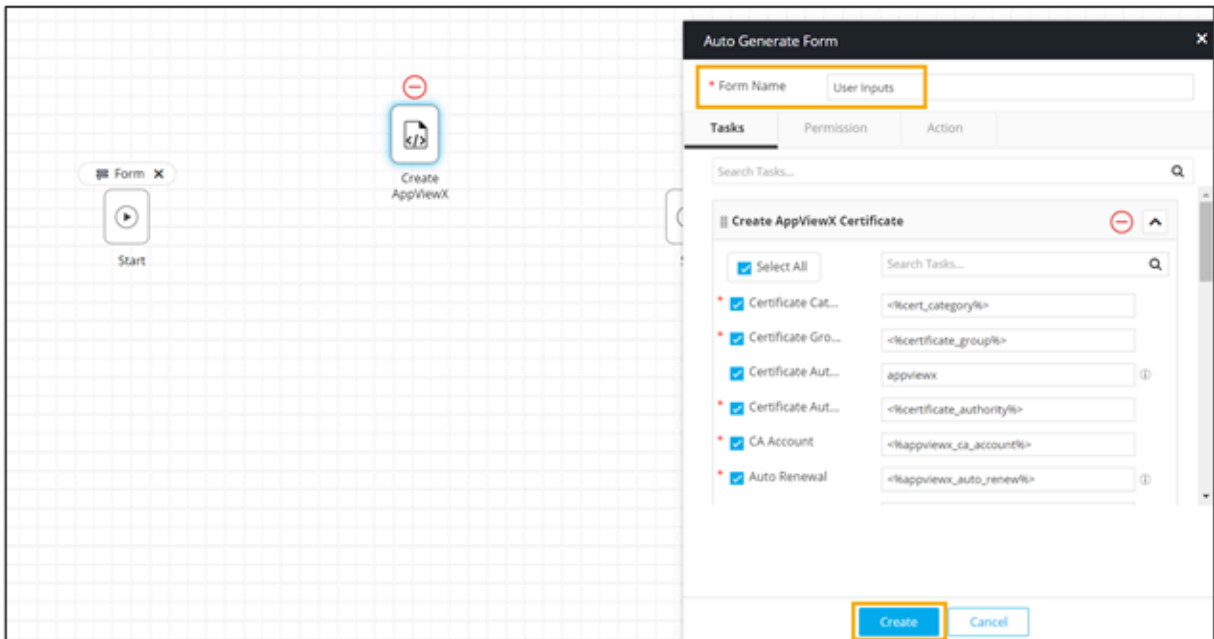


11. Click **+** above the **Create AppViewX** task to auto-populate the form fields.

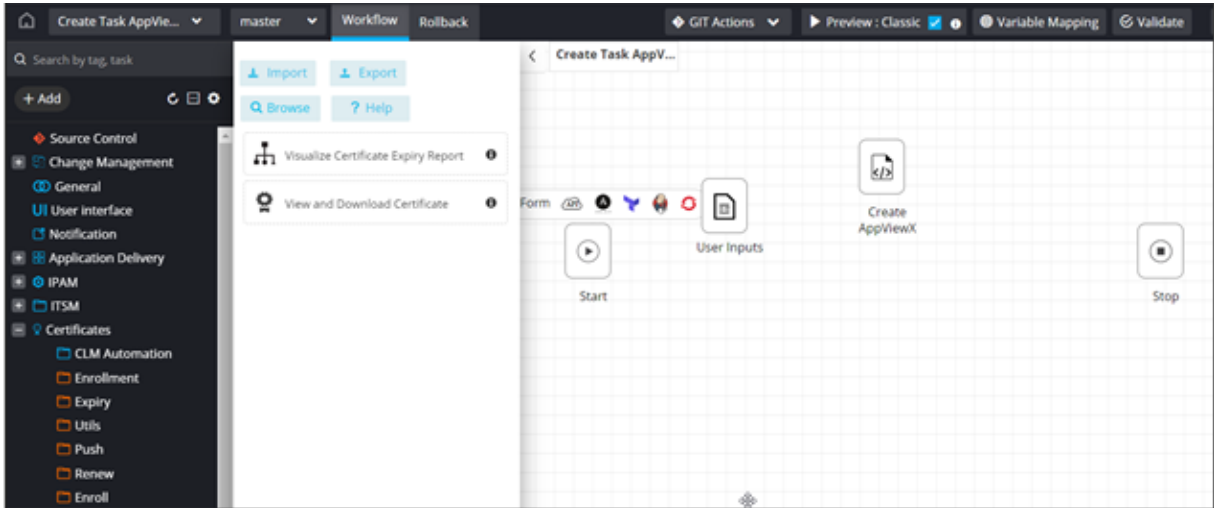


12. Select the fields required in the input form.

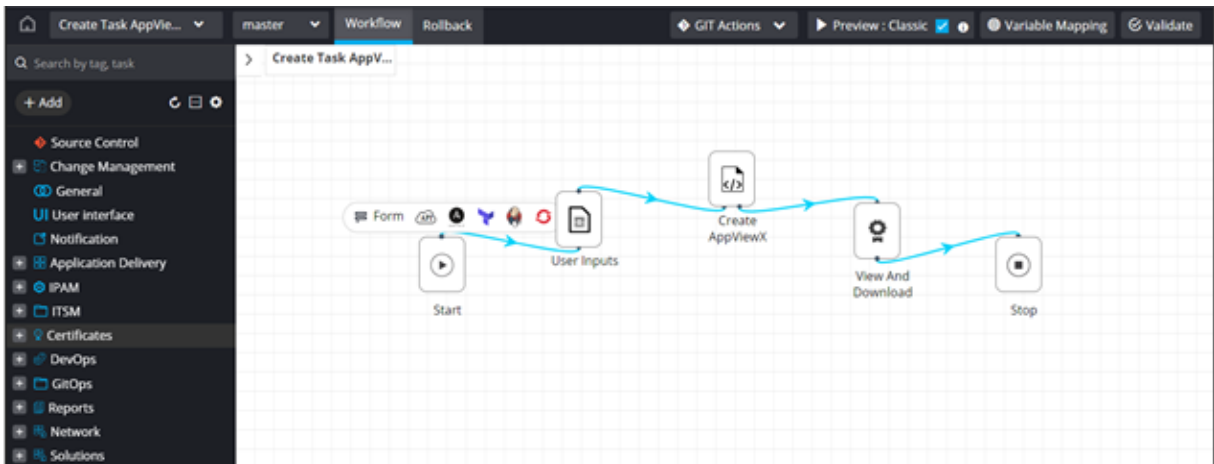
13. Provide a **Form Name** and click **Create**.



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 screenshot shows a 'Create AppViewX Certificate' form within a workflow editor. The form has the following fields and values:




- Certificate Category:** Server
- Certificate Group:** Select
- Certificate Authority:** AppViewX
- CA Account:** Select
- Auto Renewal:** False
- Renew Before (days):** (empty)
- Description:** Enter text...
- Common Name:** (empty)
- Subject Alternative Name:** None Selected
- DNS:** (empty)
- IP Address:** (empty)
- Organization:** AppViewX Inc.






Buttons at the bottom include 'Next', 'Save draft', and 'Cancel'. The left sidebar shows a 'Form' icon and a search bar.

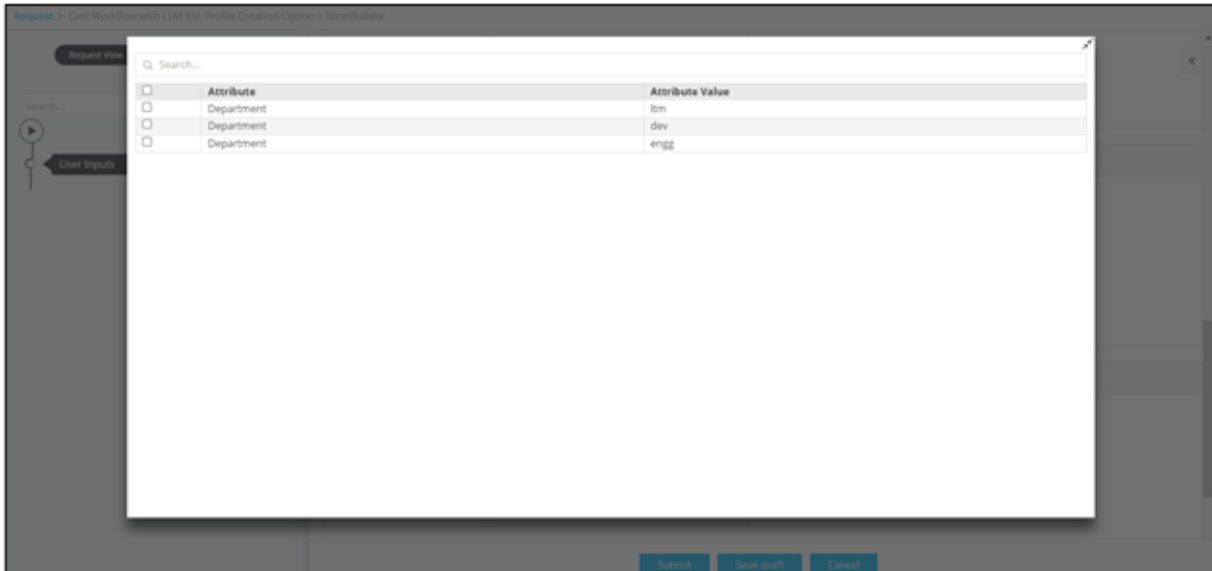
The following table describes the field information in the **User Inputs** form when the **Create AppViewX Certificate** task is selected:

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 the Email 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
	  <p>Note: To retrieve the types of keys that can be availed, click  .</p>
*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.



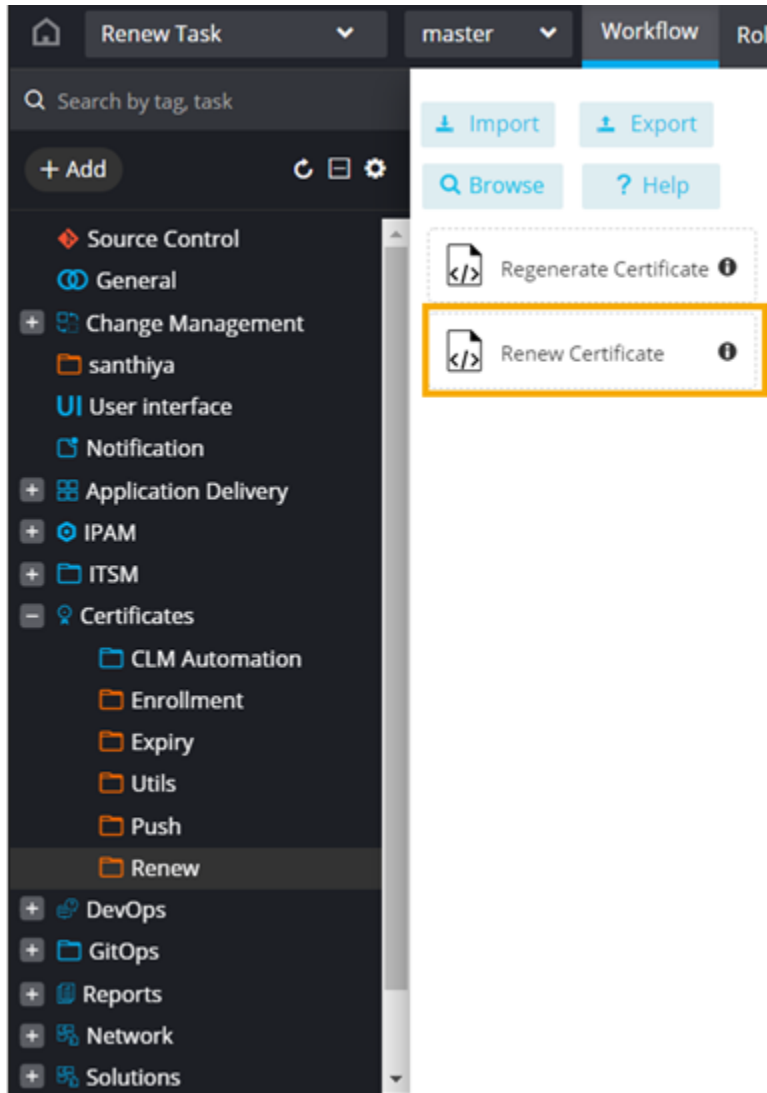
Renew Tasks

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

- [Renew Task](#)
- [Regenerate Task](#)

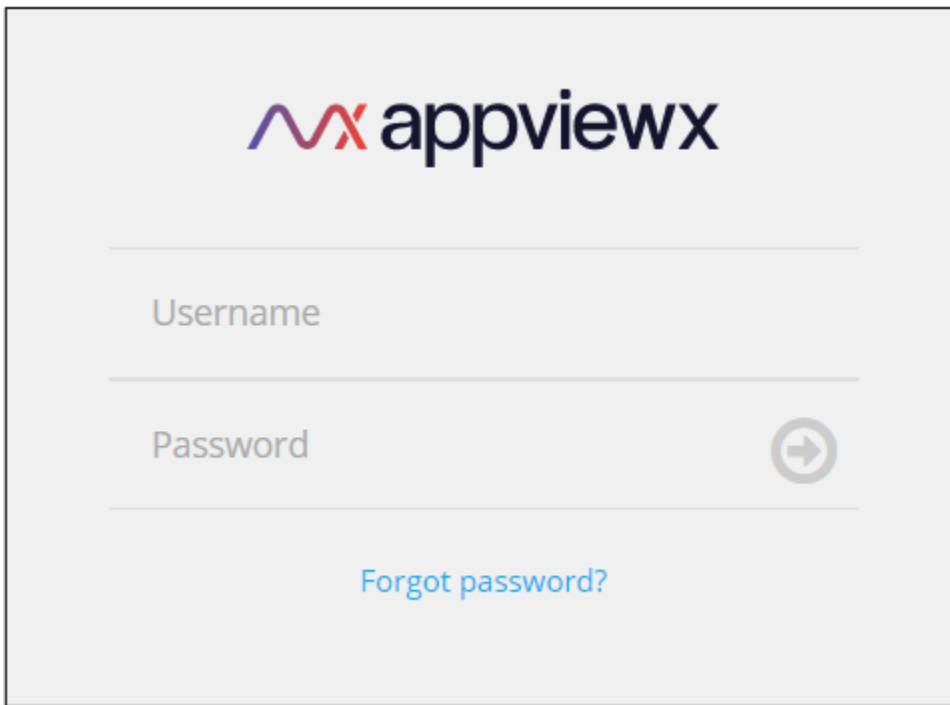
Renew Task


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

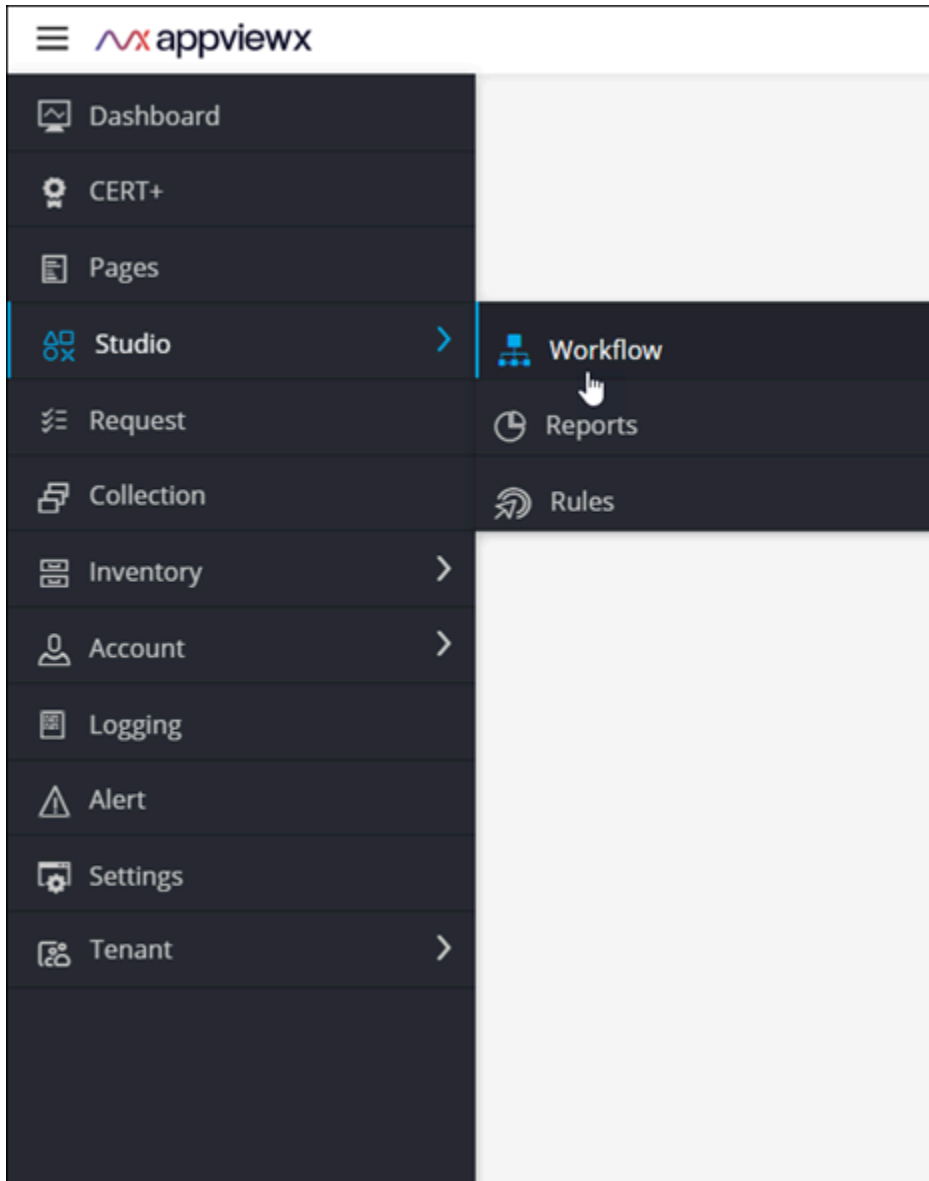


To design a custom workflow using the **Renew** task:

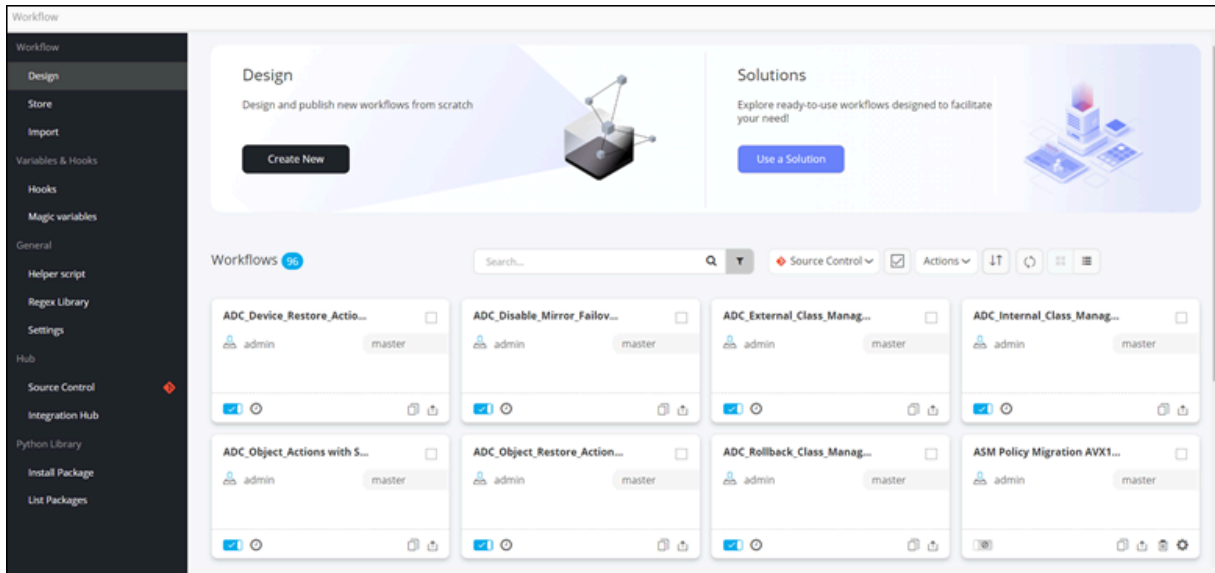
1. Log into AppViewX with valid credentials.

A screenshot of the AppViewX login interface. At the top center is the AppViewX logo, consisting of a stylized 'VX' in red and blue followed by the text 'appviewx' in a dark blue sans-serif font. Below the logo are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. To the right of the password field is a circular button with a right-pointing arrow. Below the password field is a blue link that says 'Forgot password?'. The entire login form is enclosed in a thin black border.

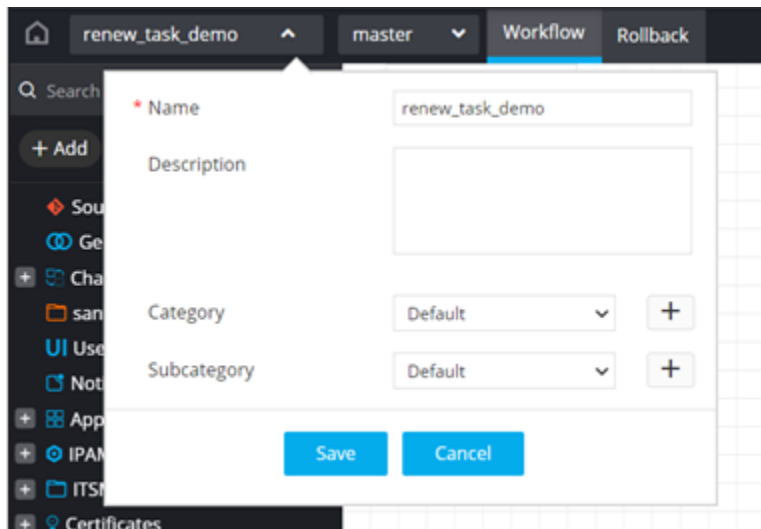
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



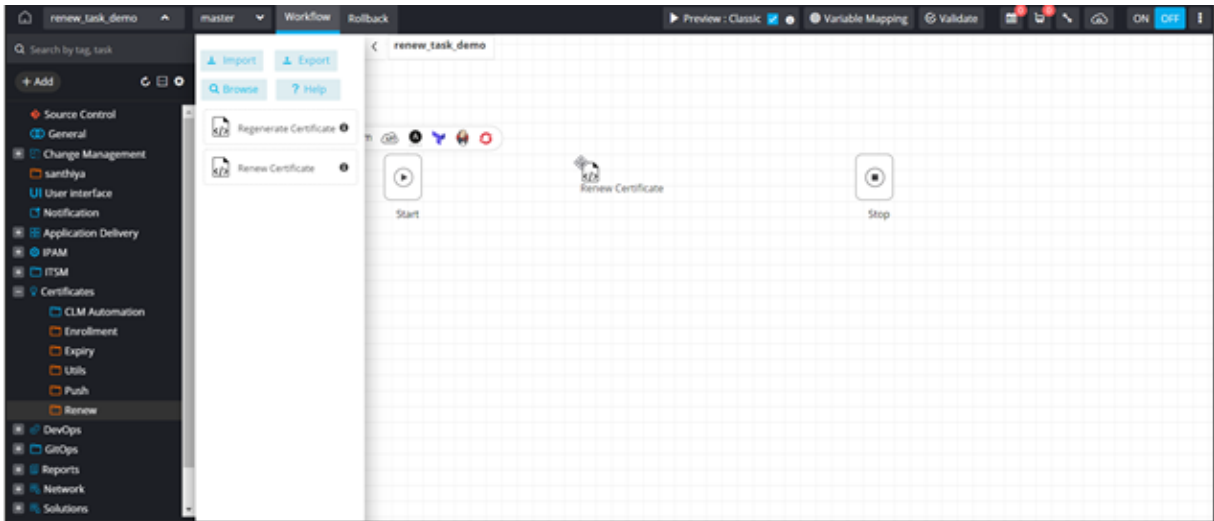
The **Workflow** inventory page is displayed.



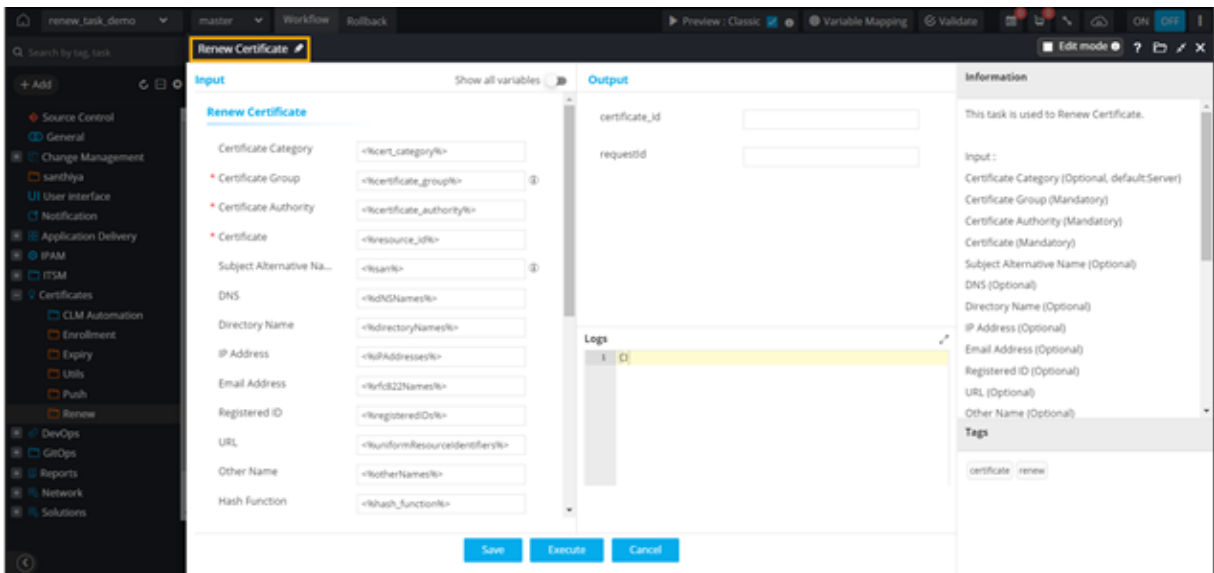
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



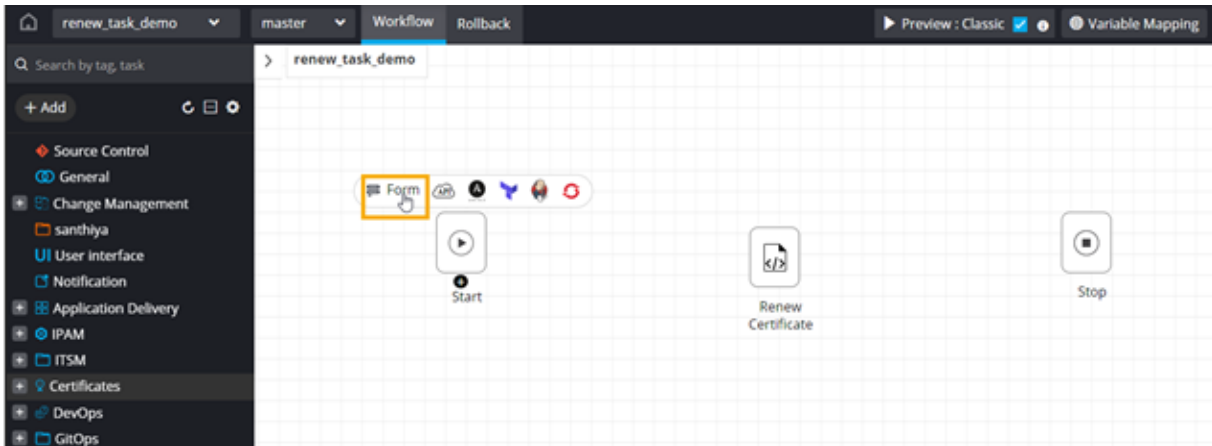
7. From the **Certificates** folder, under **Renew**, drag and drop the **Renew Certificate** task.



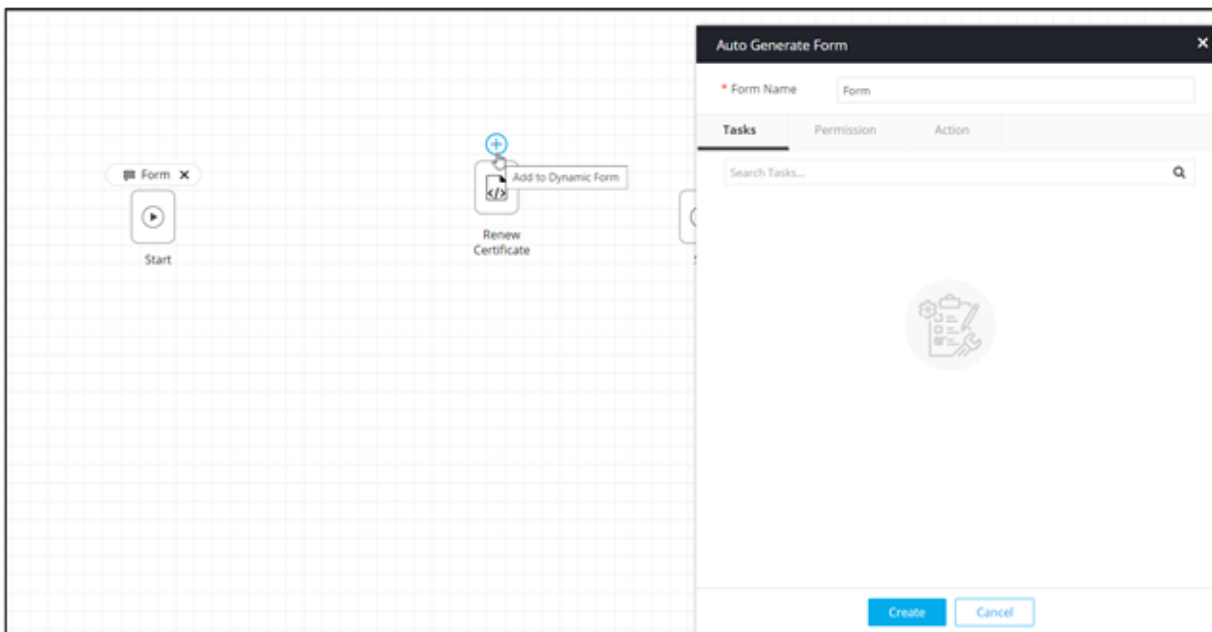
This task can be used to renew certificates.



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

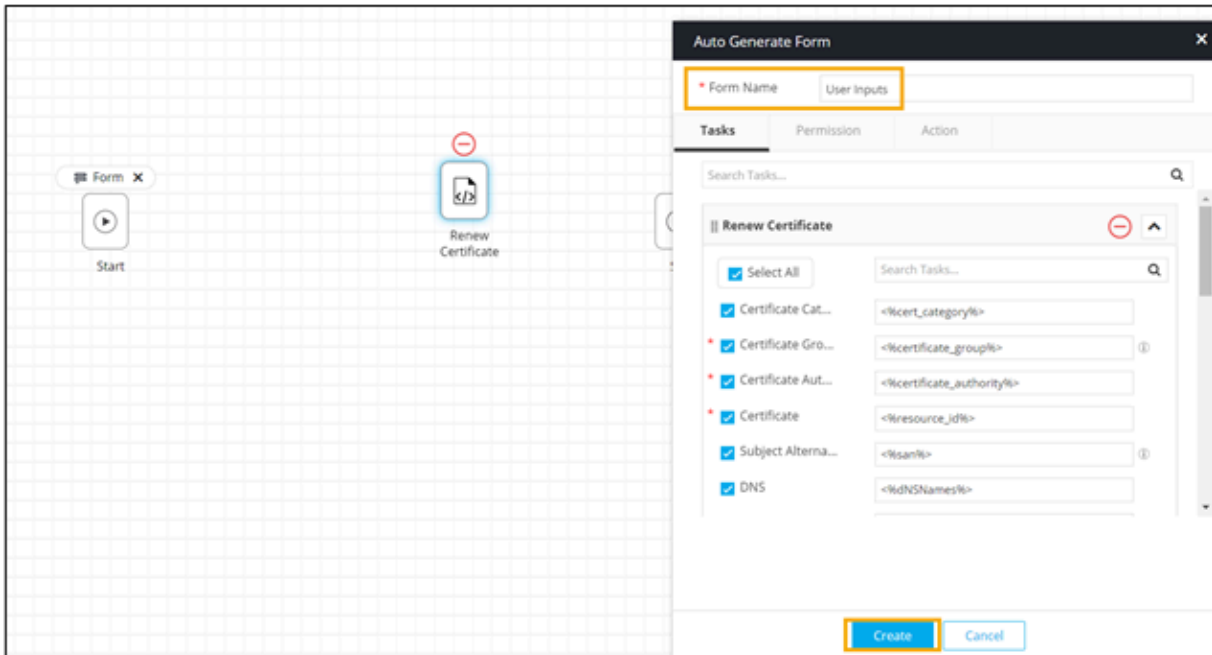


9. Click  above the **Renew Certificates** task to auto-populate the form fields.

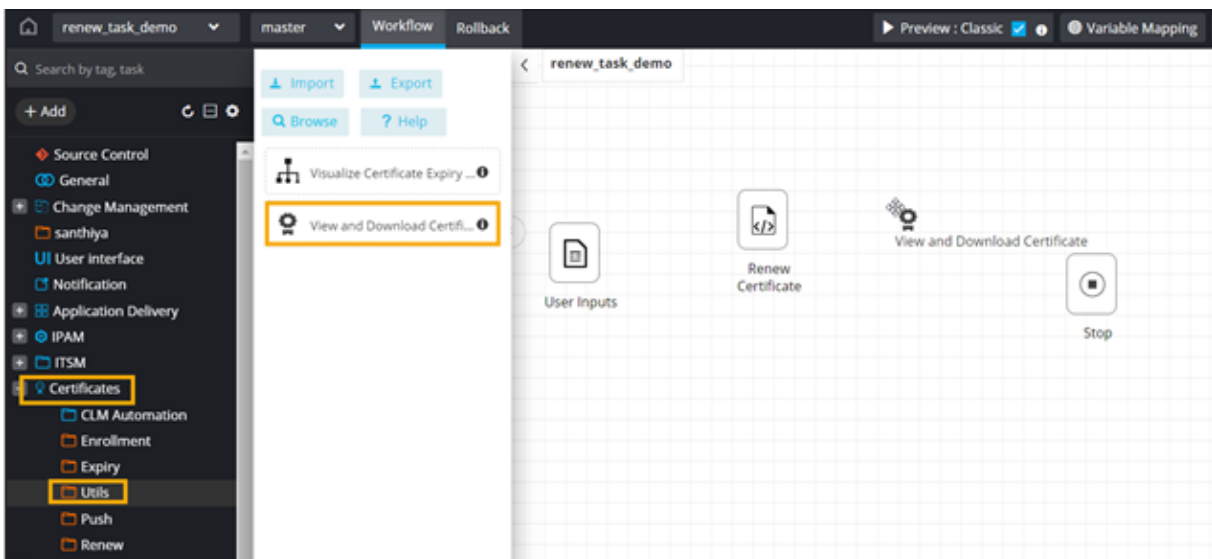


10. Select the fields required in the input form.

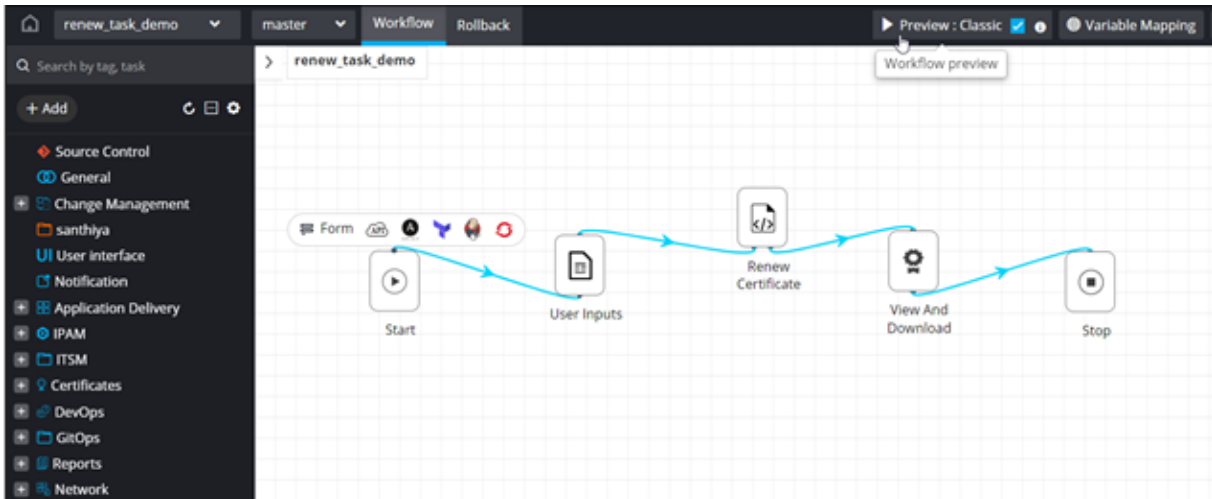
11. Provide a **Form Name** and click **Create**.



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:

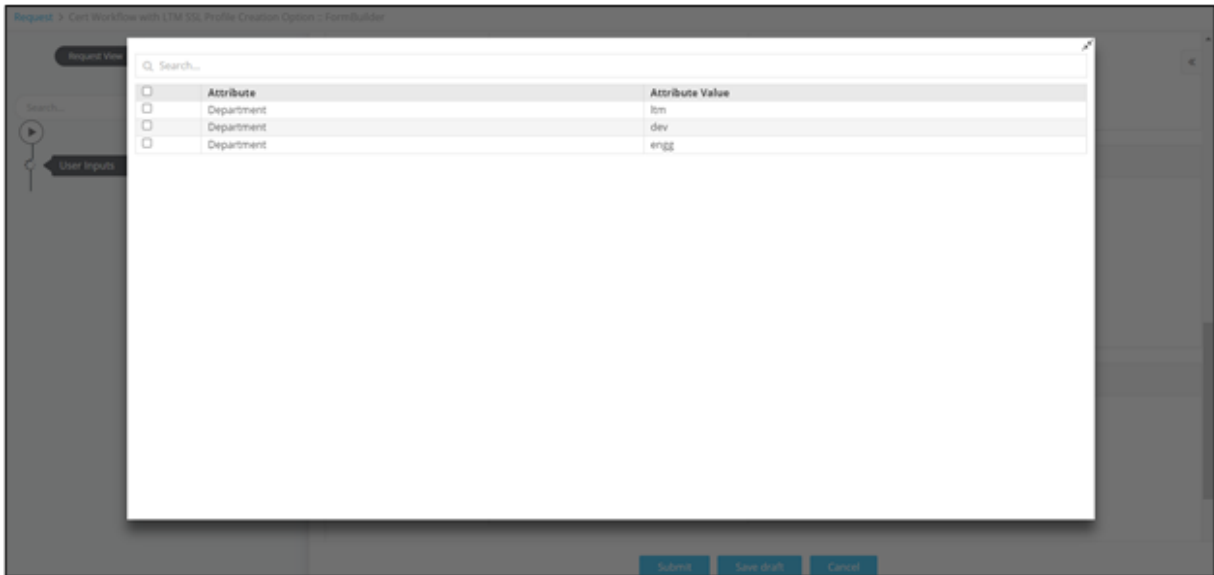
Field	Description
Certificate Category	Select the Certificate Category from the options available in the dropdown. <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 5px; background-color: #e6f2ff;">  Note: Server is the default selection. </div>
*Certificate Group	Select the Certificate 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 .

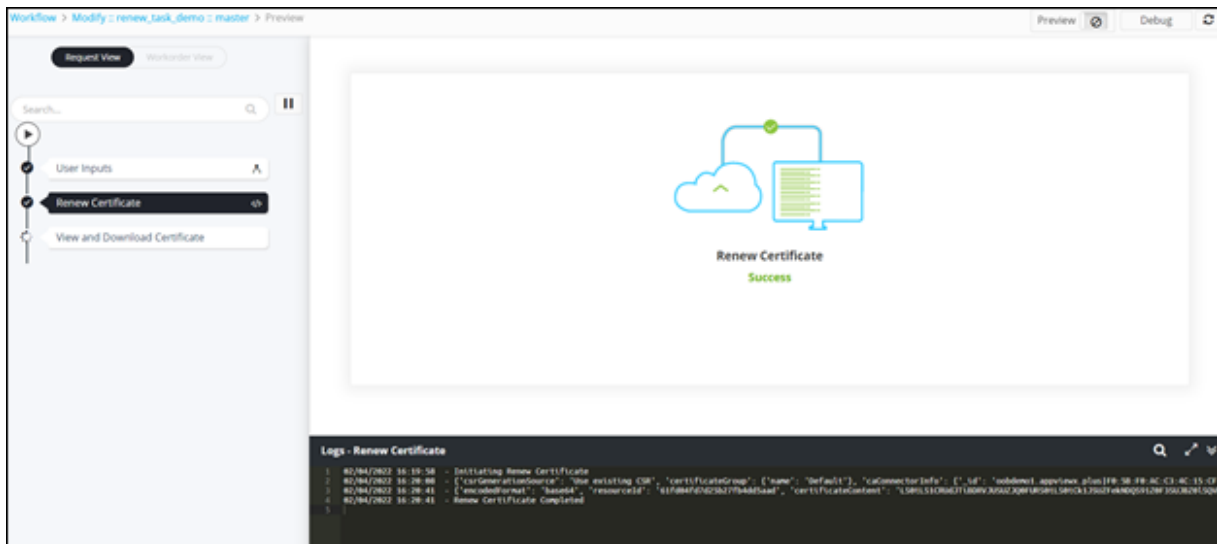
15. To edit the value of a particular attribute, select the attribute in the grid and click .

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**.

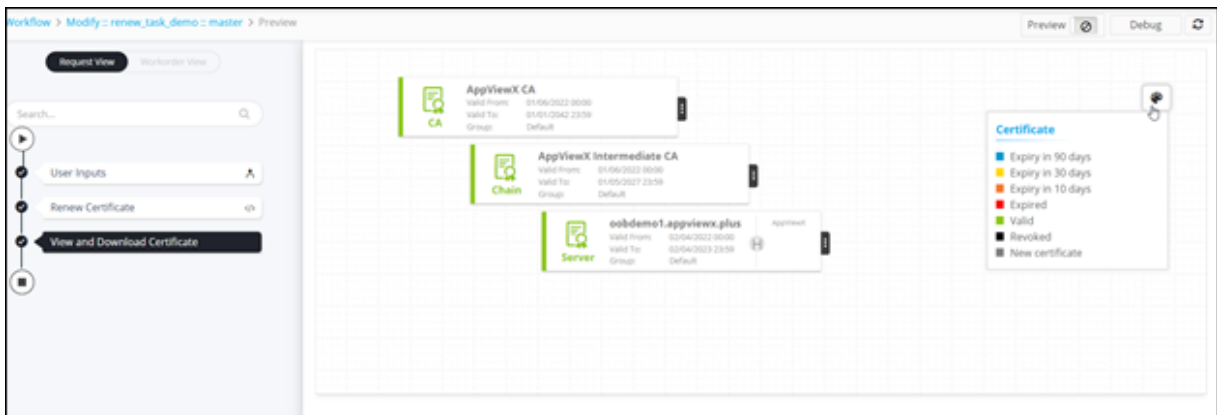
Certificate renewed successfully.



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**.

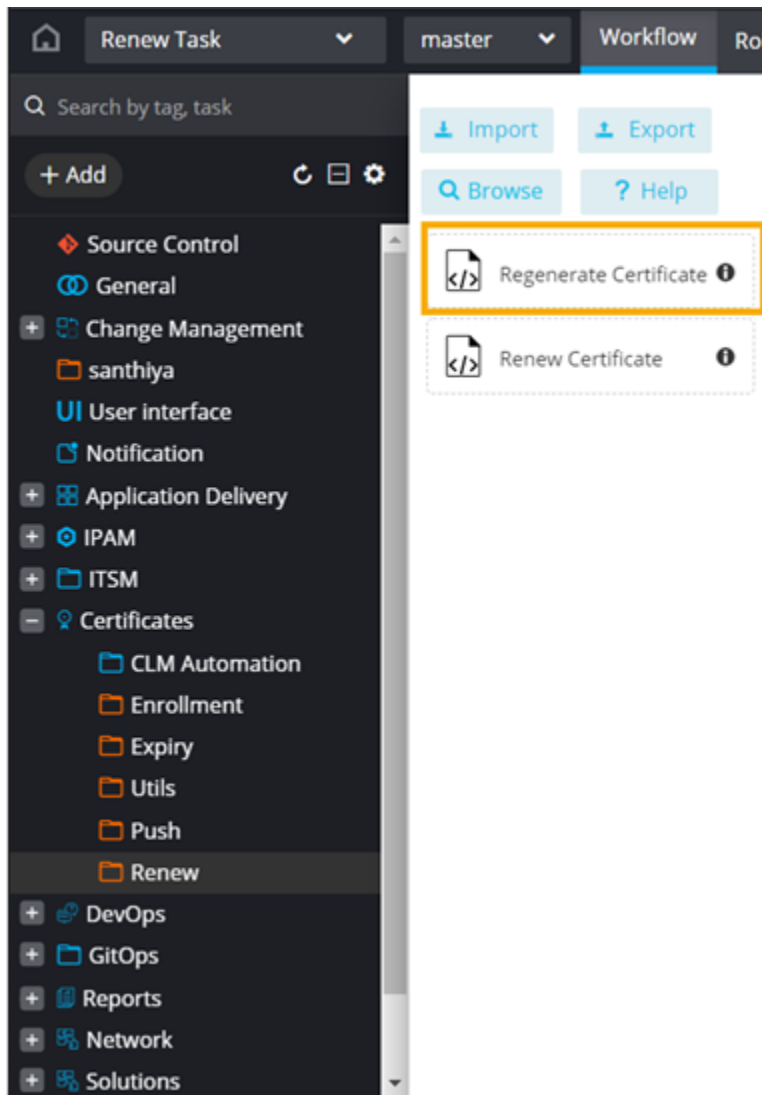




Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.

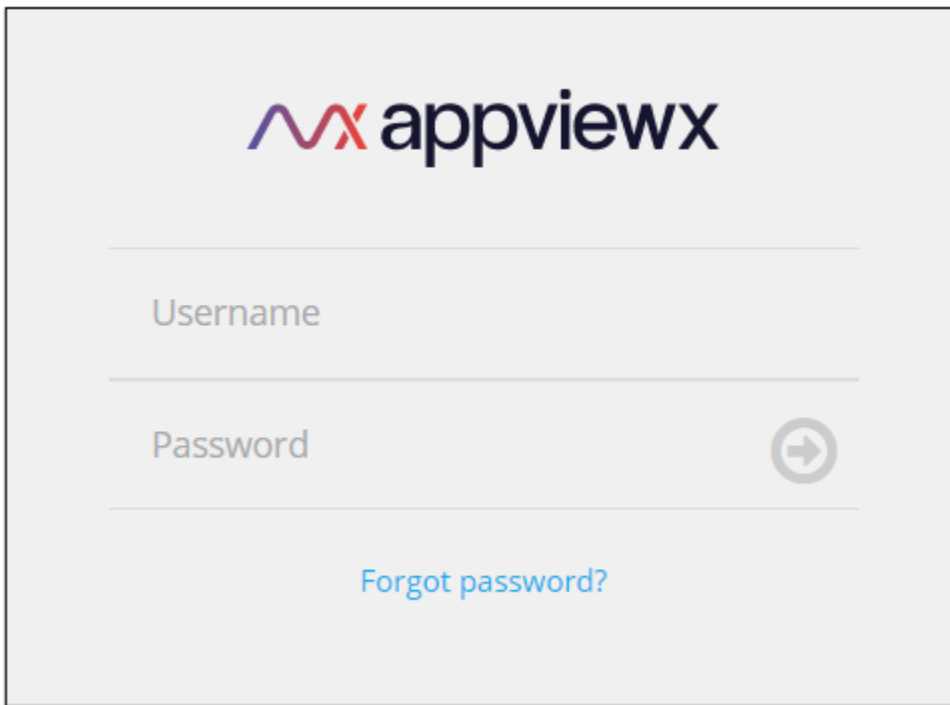
Regenerate Task

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




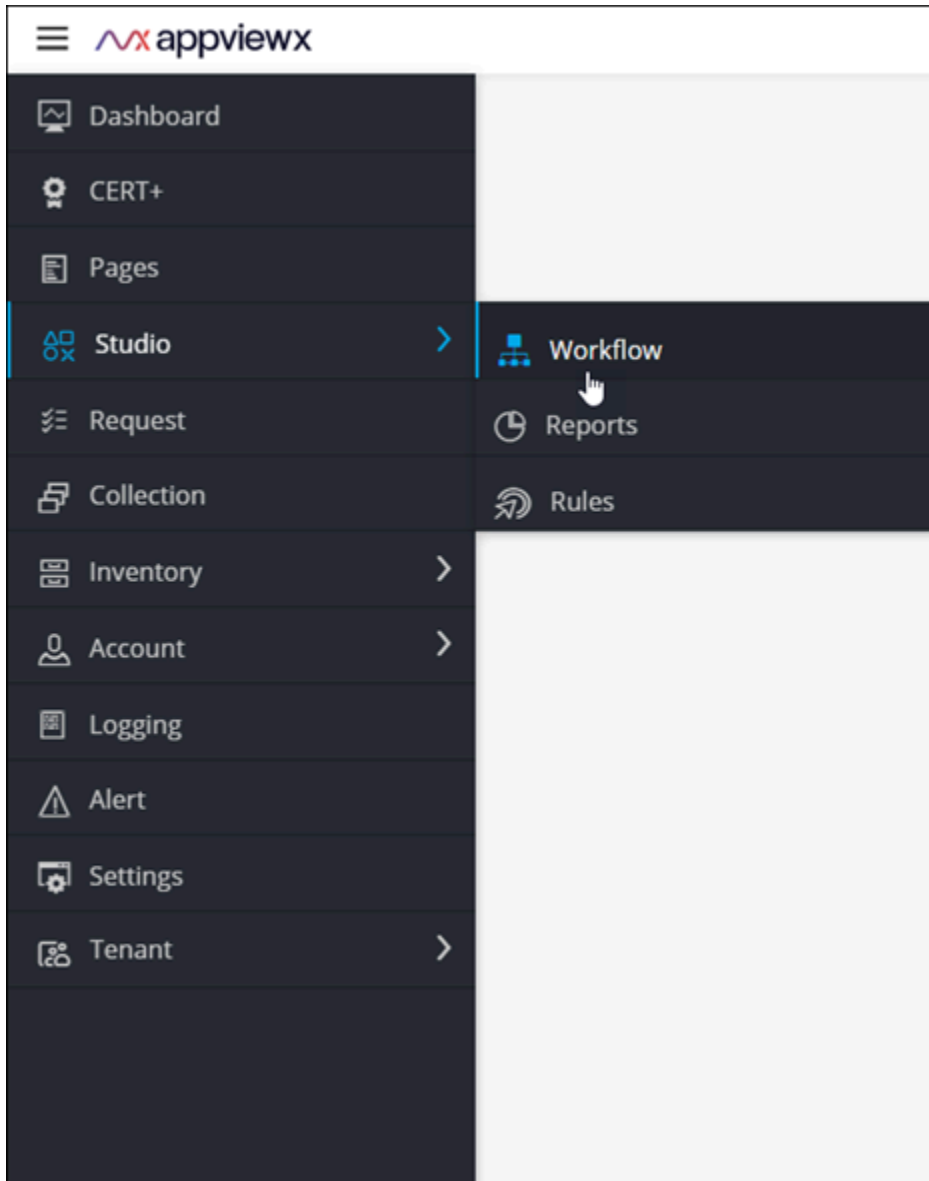
To design a custom workflow using the **Regenerate** task:

1. Log into AppViewX with valid credentials.

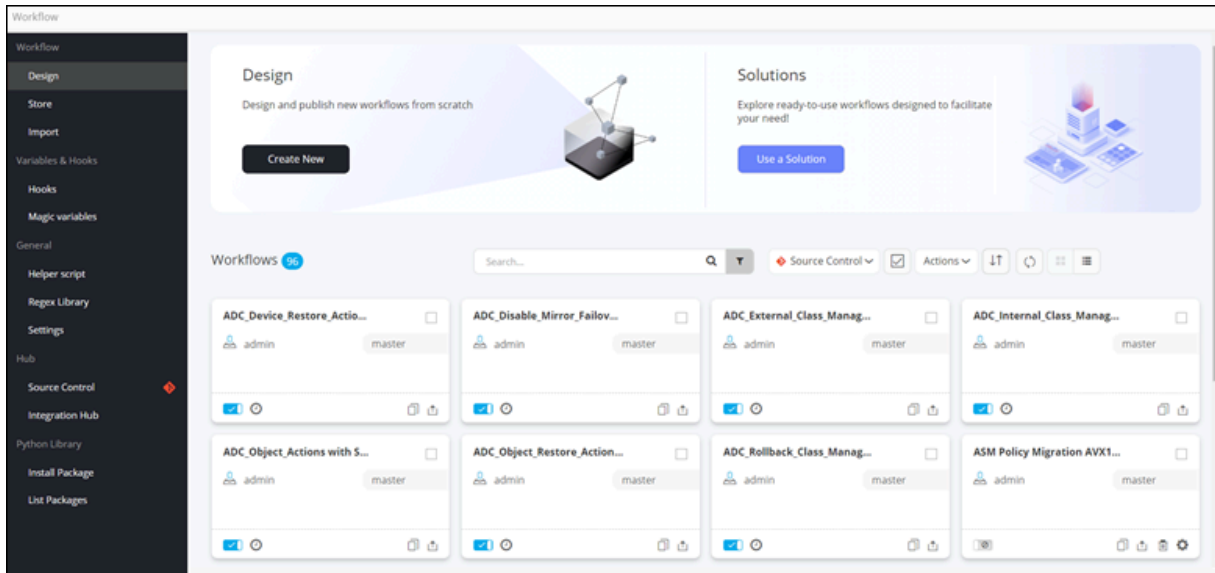


The image shows a login form for AppViewX. At the top, the AppViewX logo is displayed, consisting of a stylized 'VX' in red and blue followed by the text 'appviewx'. Below the logo are two input fields: 'Username' and 'Password'. The 'Password' field has a circular icon with a right-pointing arrow on its right side. Below the input fields is a link that says 'Forgot password?' in blue text.

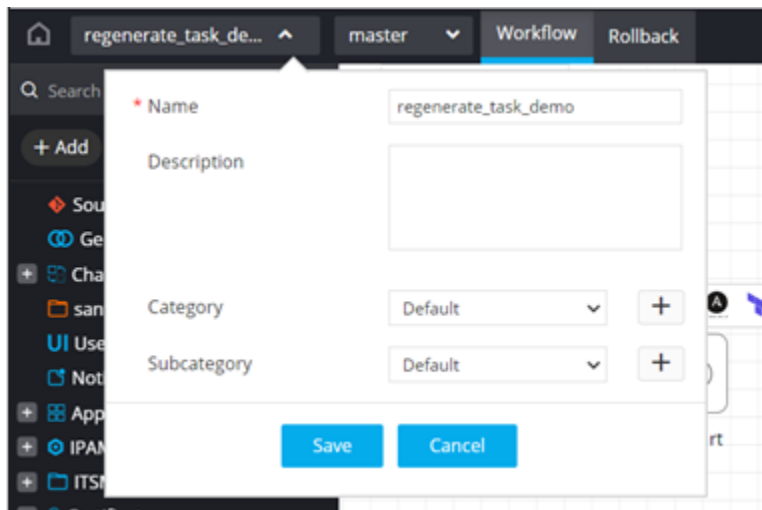
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



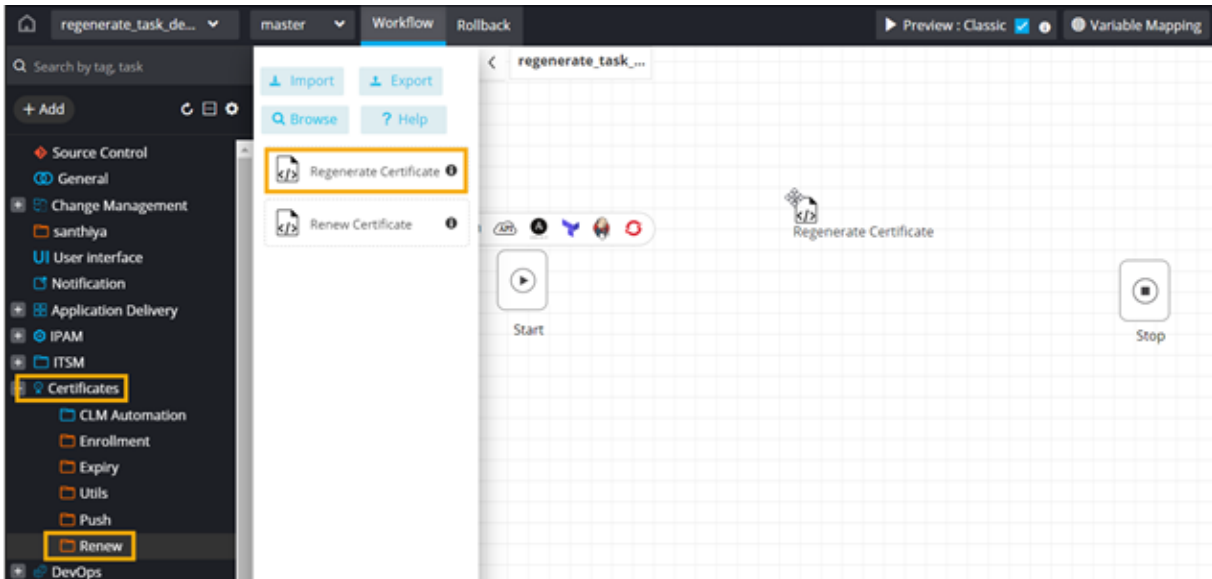
The **Workflow** inventory page is displayed.



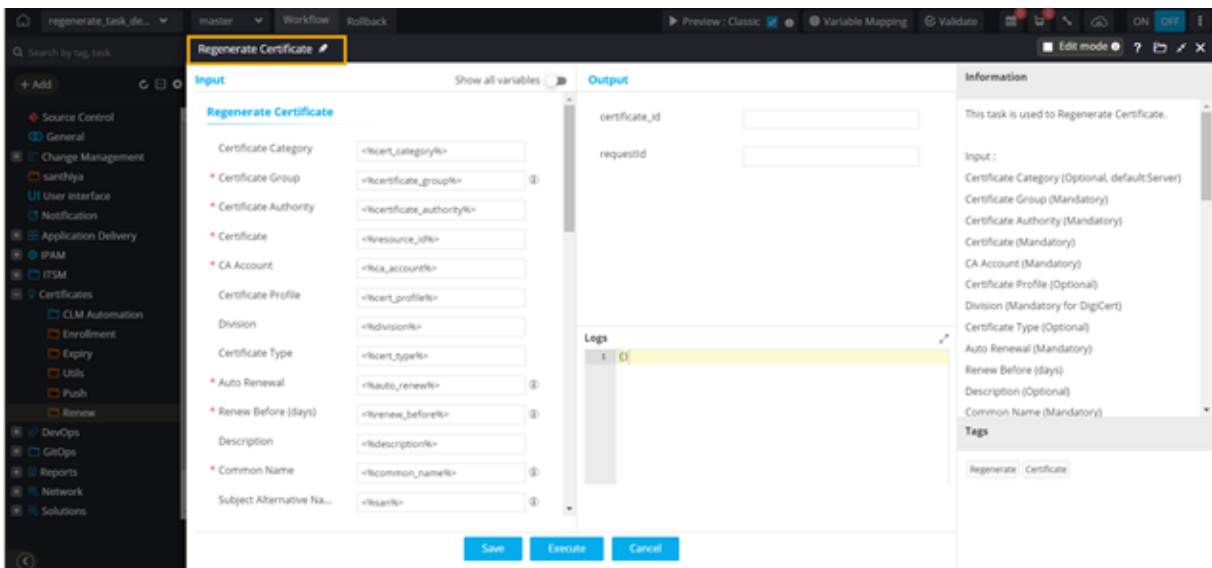
4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.



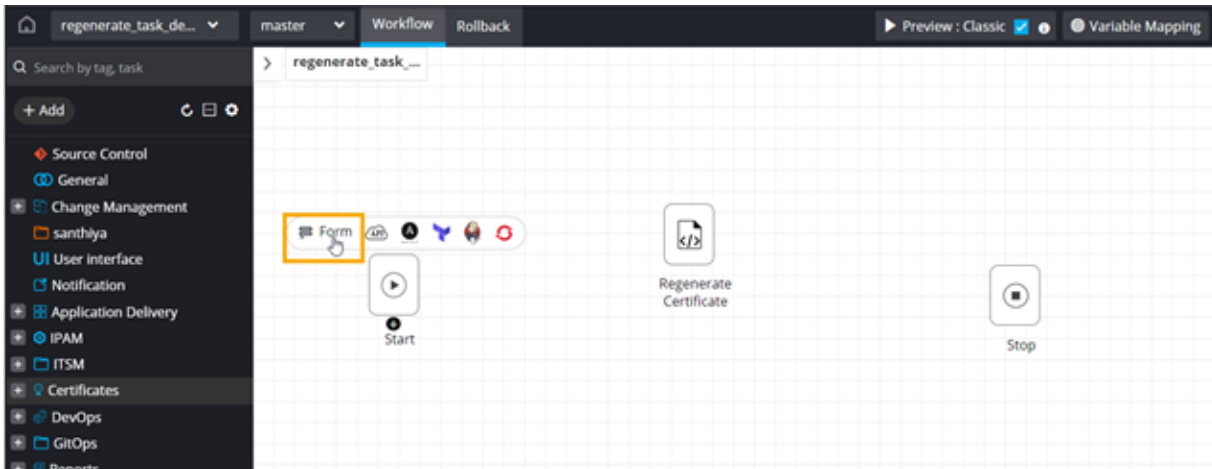
7. From the **Certificates** folder, under **Renew**, drag and drop the **Regenerate Certificate** task.



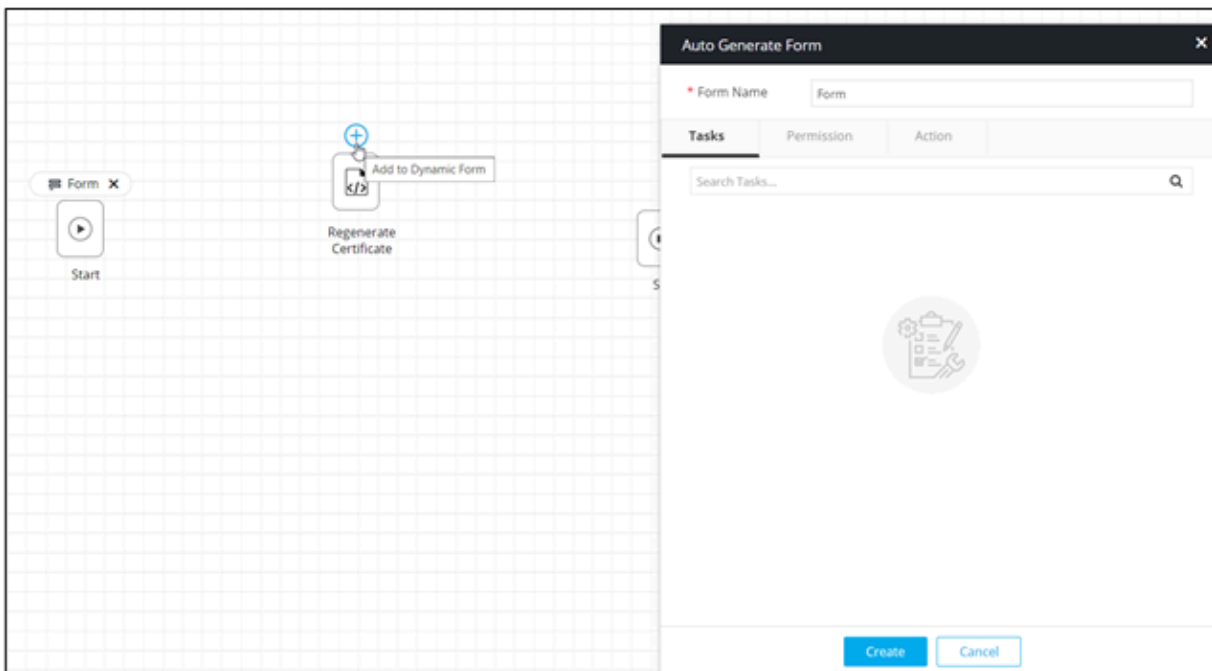
This task can be used to regenerate certificates.



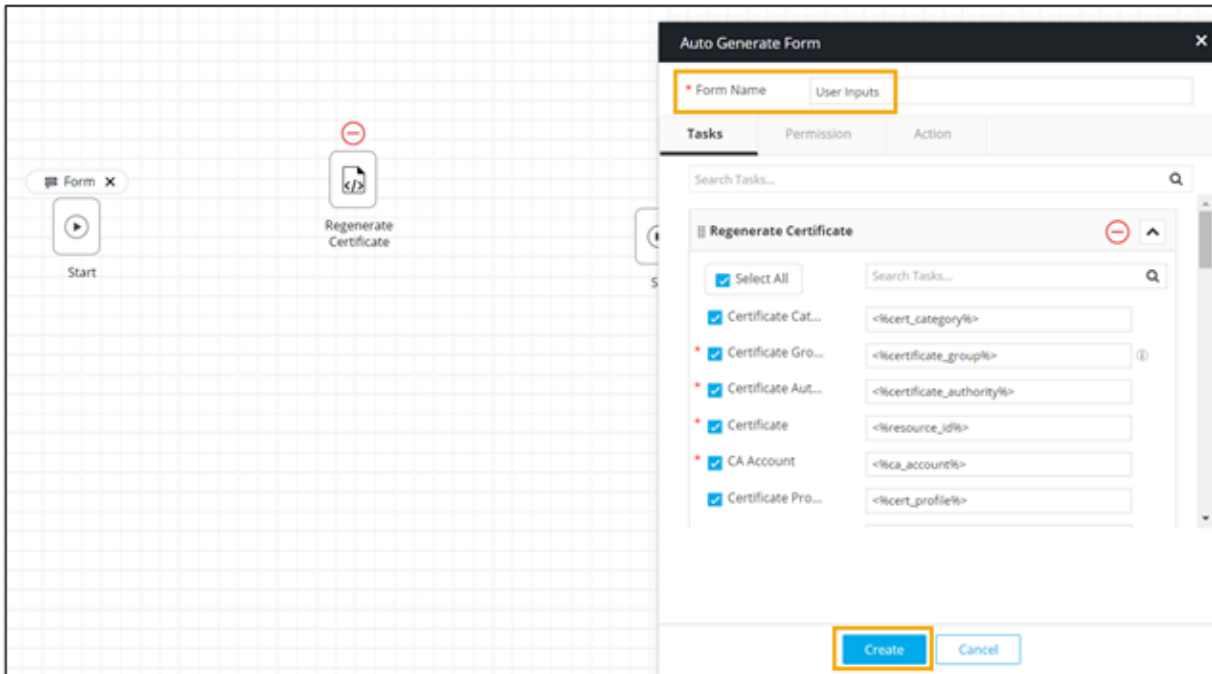
8. To auto-generate a form for this workflow, click **Form** above the **Start** task.



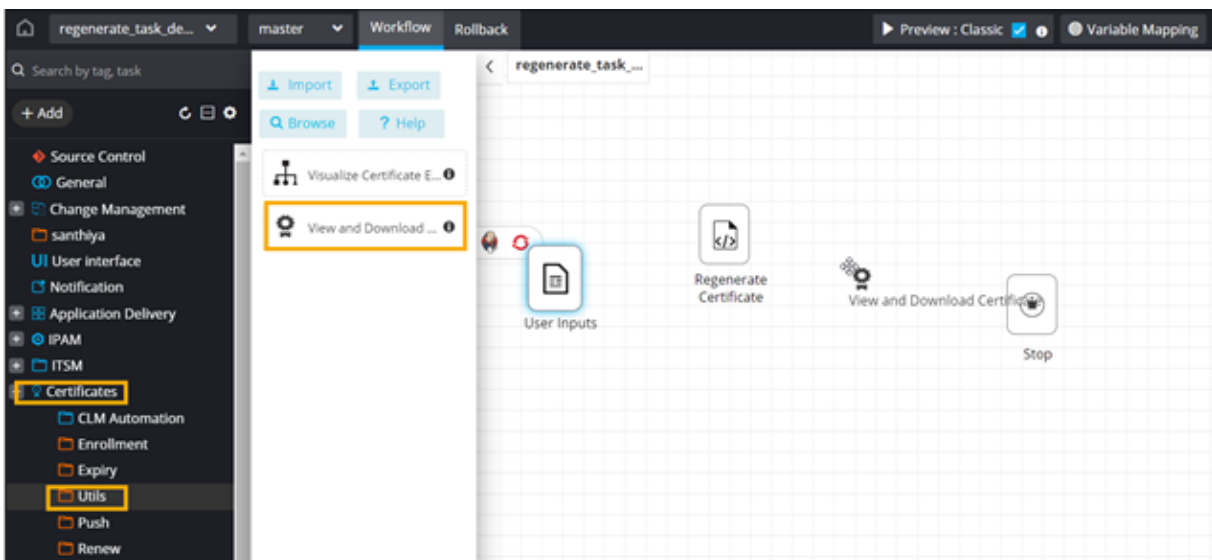
9. Click  above the **Regenerate Certificates** task to auto-populate the form fields.



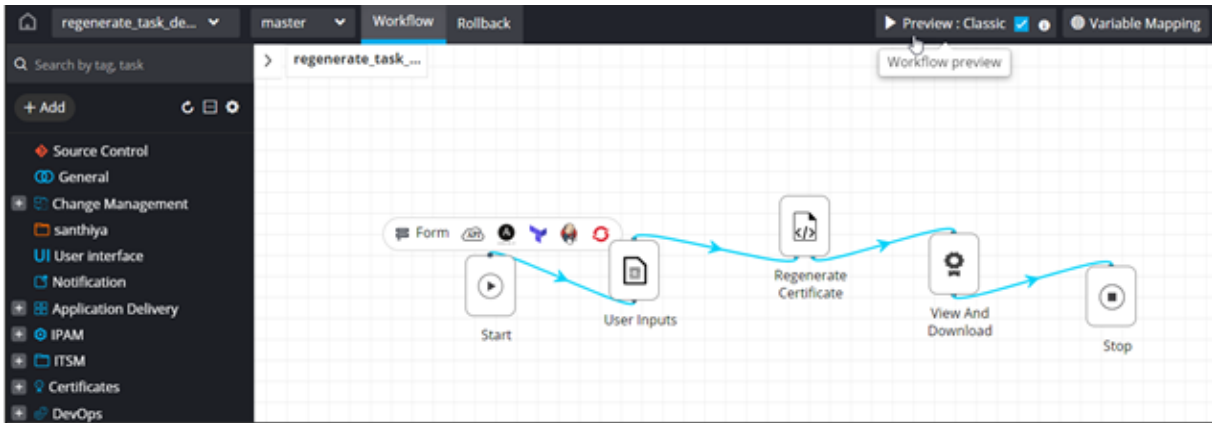
10. Select the fields required in the input form.
 11. Provide a **Form Name** and click **Create**.



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.









Regenerate Certificate



- Certificate Category: Server
- *Certificate Group: Select
- *Certificate Authority: Select
- *Certificate: Select
- *CA Account: Select
- *Auto Renewal: False
- Description: Enter text...
- *Common Name:
- Subject Alternative Name: None Selected
- DNS:
- IP Address:
- Organization:






Buttons: Next, Save draft, Cancel

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  .

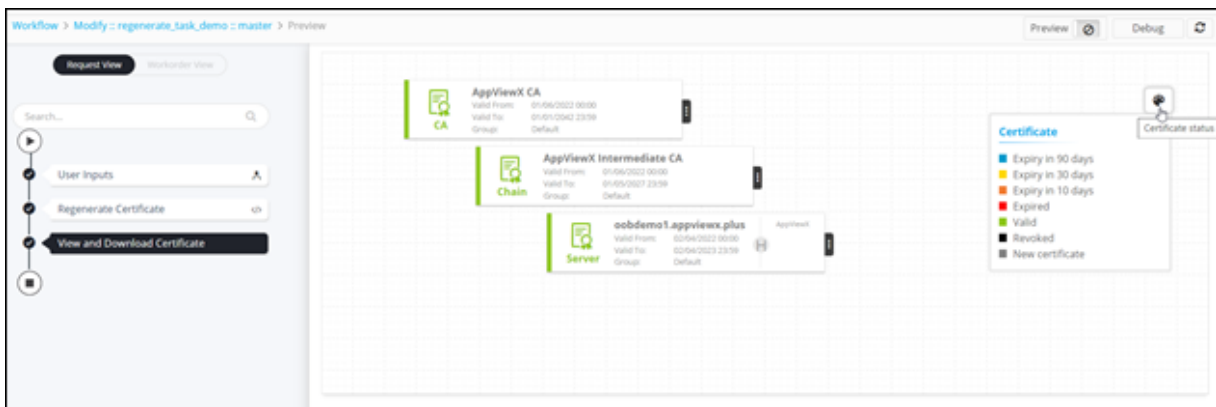
Field	Description
*Certificate Authority	Select the Certificate Authority from the options available in the dropdown.  Note: To retrieve the values in the Certificate Authority field, click  .
*Certificate	Select the Certificate from the options available in the dropdown.  Note: To retrieve the values 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. <div style="border: 1px solid #00aaff; border-radius: 10px; padding: 5px; background-color: #e6f2ff;">  Note: To retrieve the values in the Bit Length field, click . </div>
*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 .



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



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

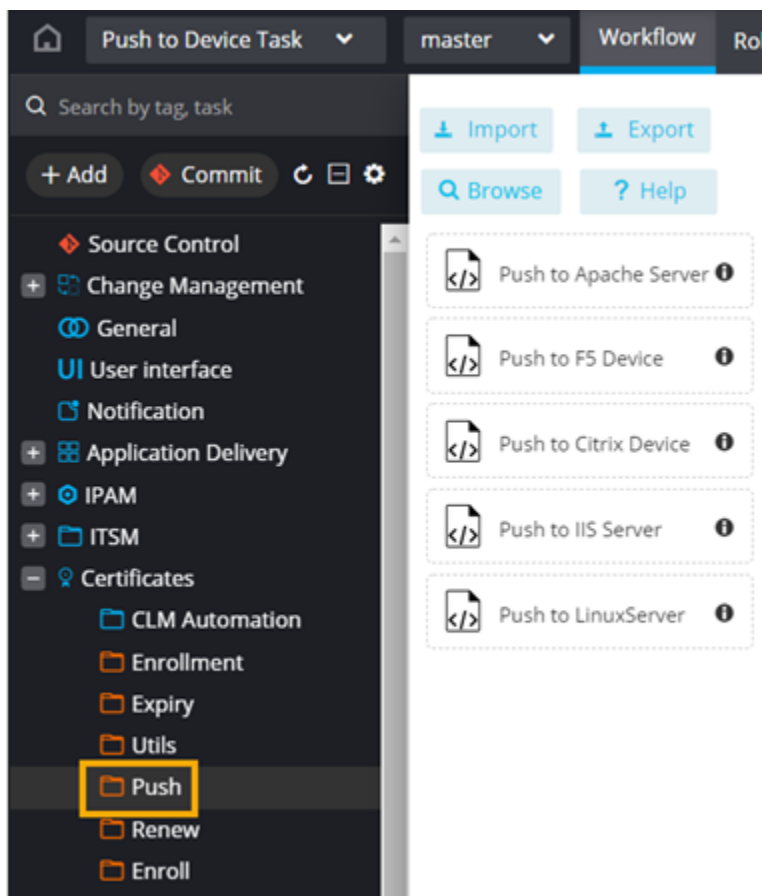




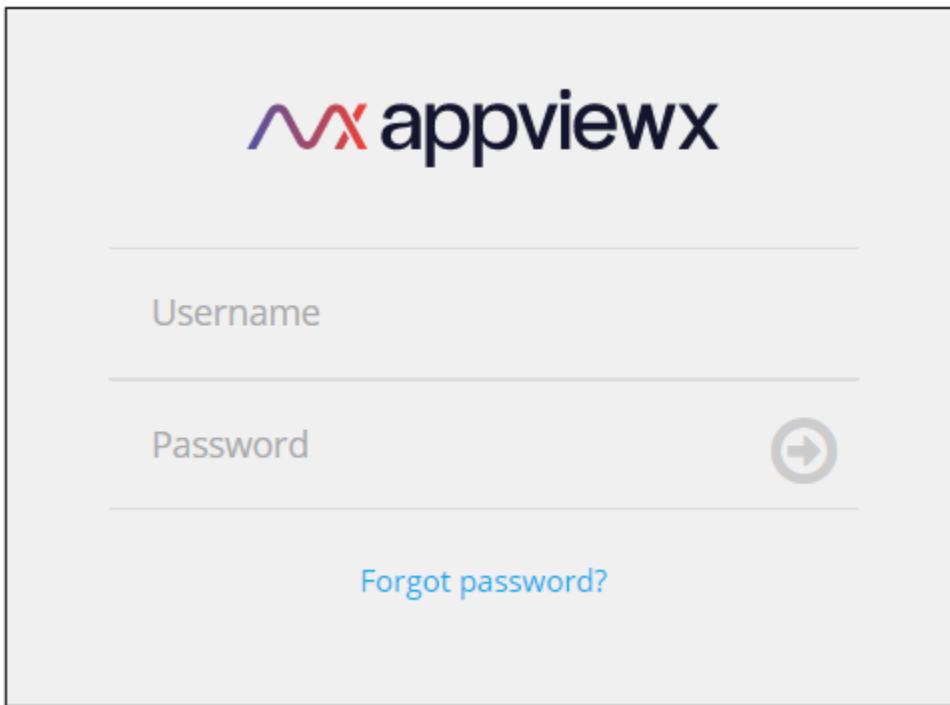
Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.


Push Tasks

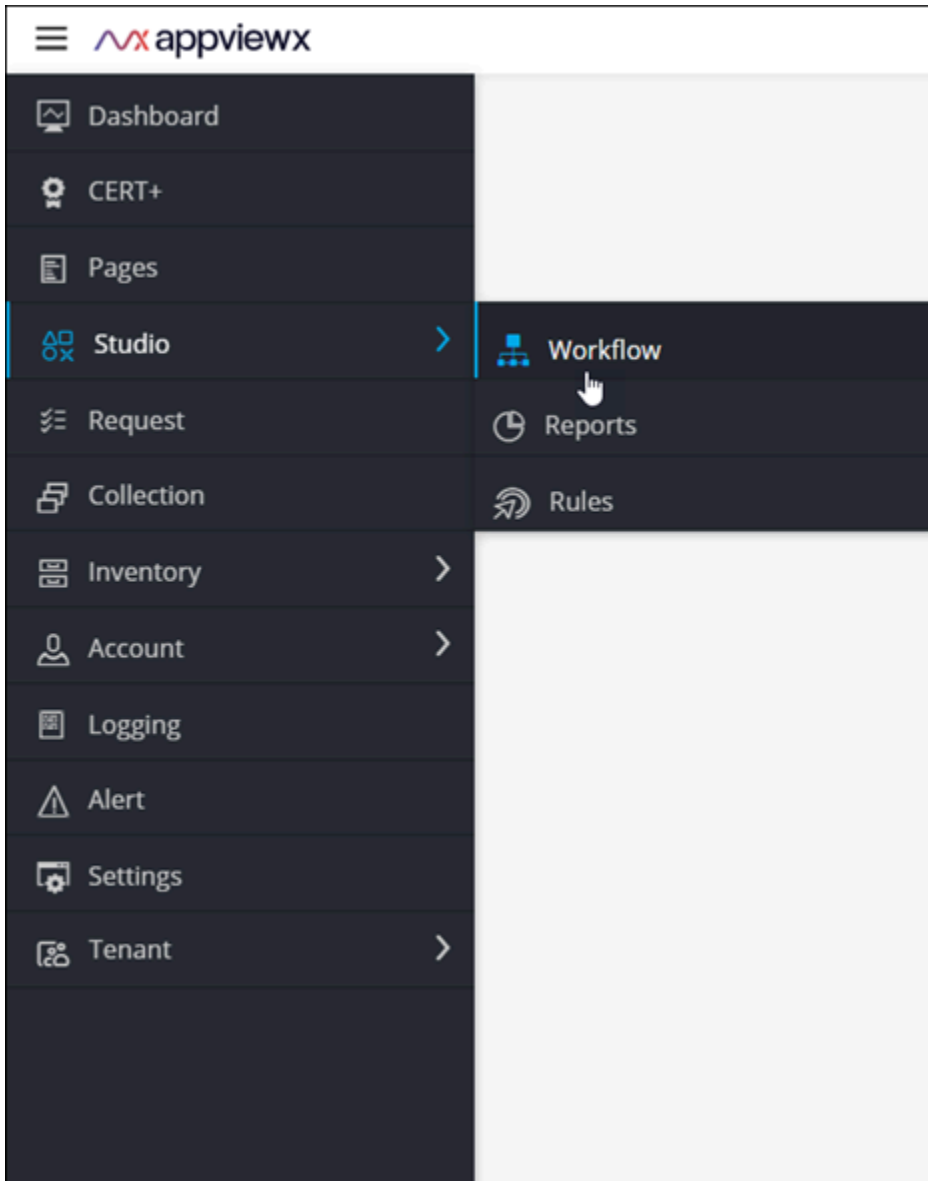
You can design a custom workflow for pushing a certificate to a device(s) or a server(s) using the prebuilt Push tasks available in the **Workflow Studio**. The OOB script task for pushing certificates to devices/servers can be found under **Certificates**, in the **Push** folder.



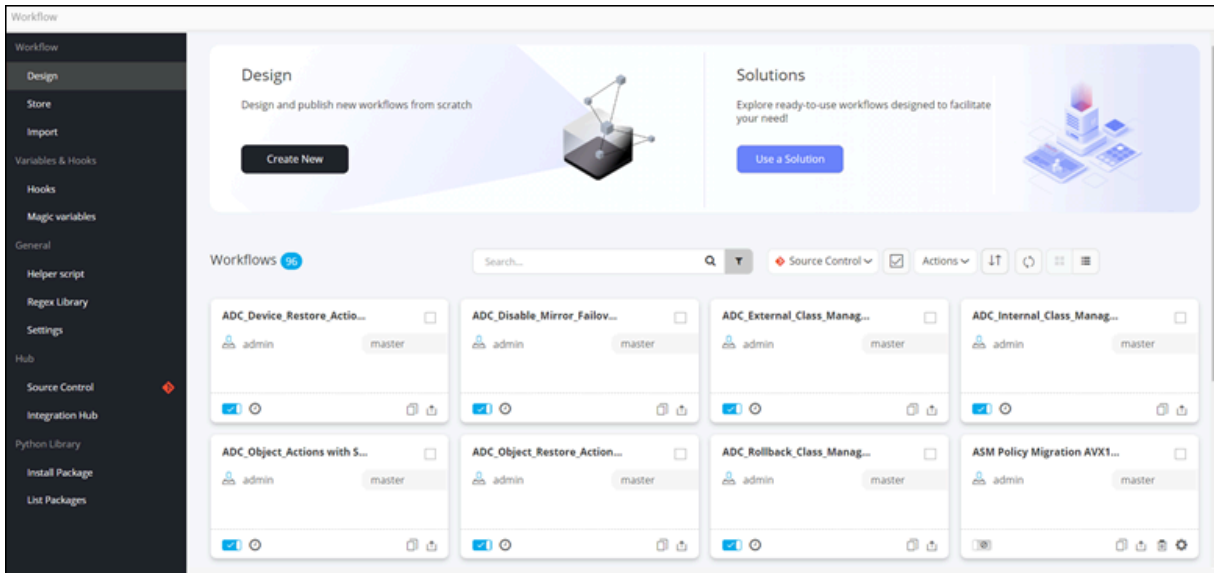
1. Log into AppViewX with valid credentials.

The image shows a login form for AppViewX. At the top center is the AppViewX logo, which consists of a stylized 'VX' in red and blue followed by the text 'appviewx' in a dark blue sans-serif font. Below the logo are two input fields. The first field is labeled 'Username' and the second is labeled 'Password'. To the right of the password field is a circular button with a right-pointing arrow. Below the password field is a link that says 'Forgot password?' in a blue color.

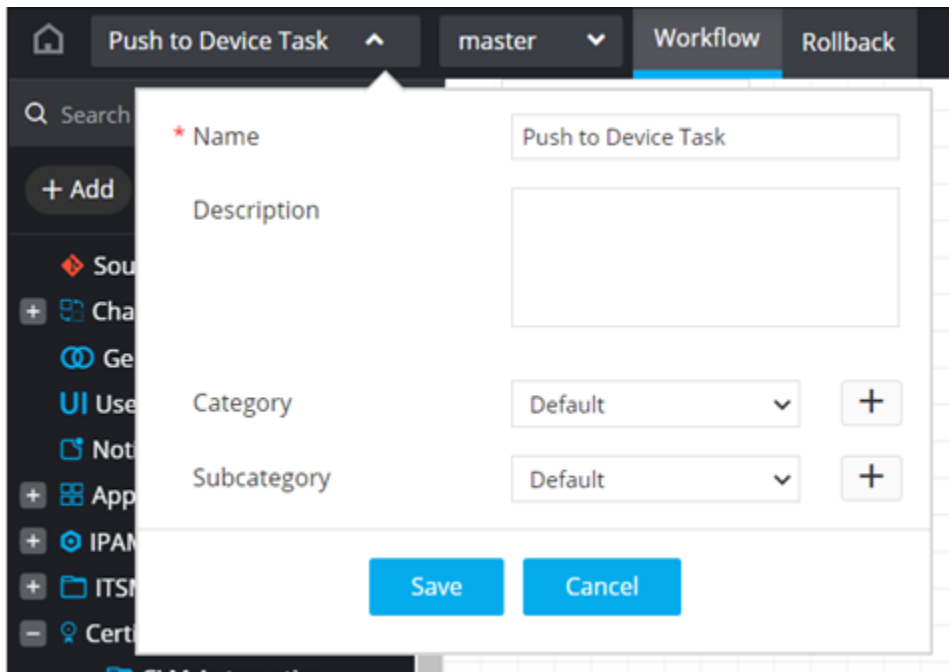
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



The **Workflow** inventory page is displayed.

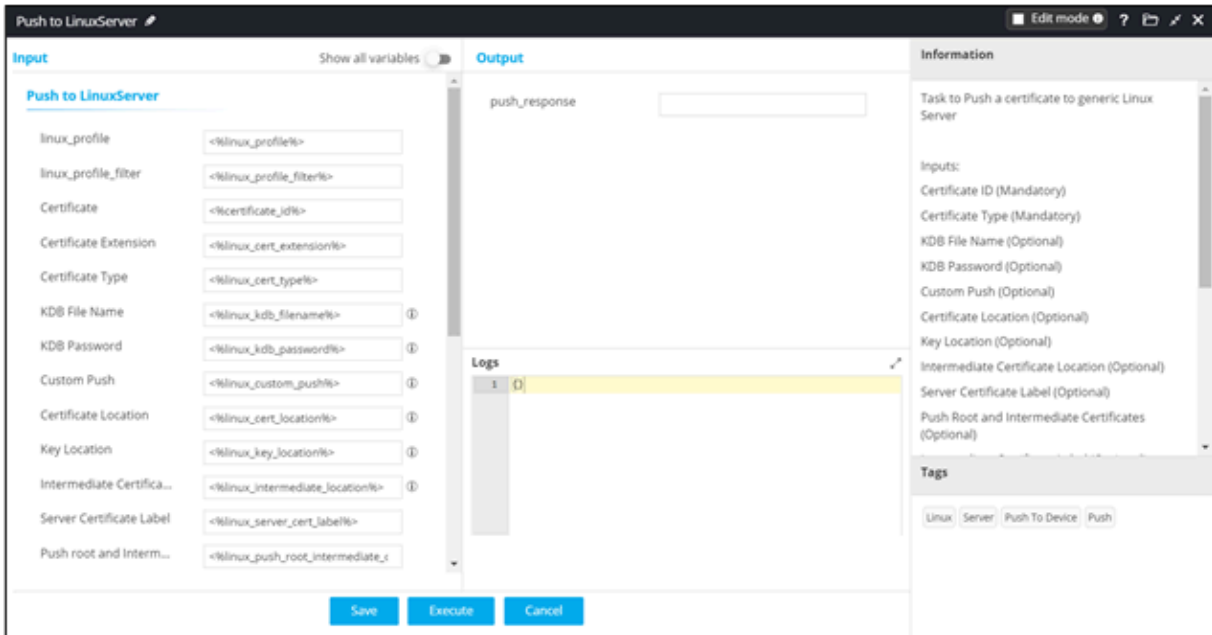


4. On the **Workflow** inventory page, click **Create New**.
5. Provide a suitable **Name** for the workflow.
6. Click **Save**.

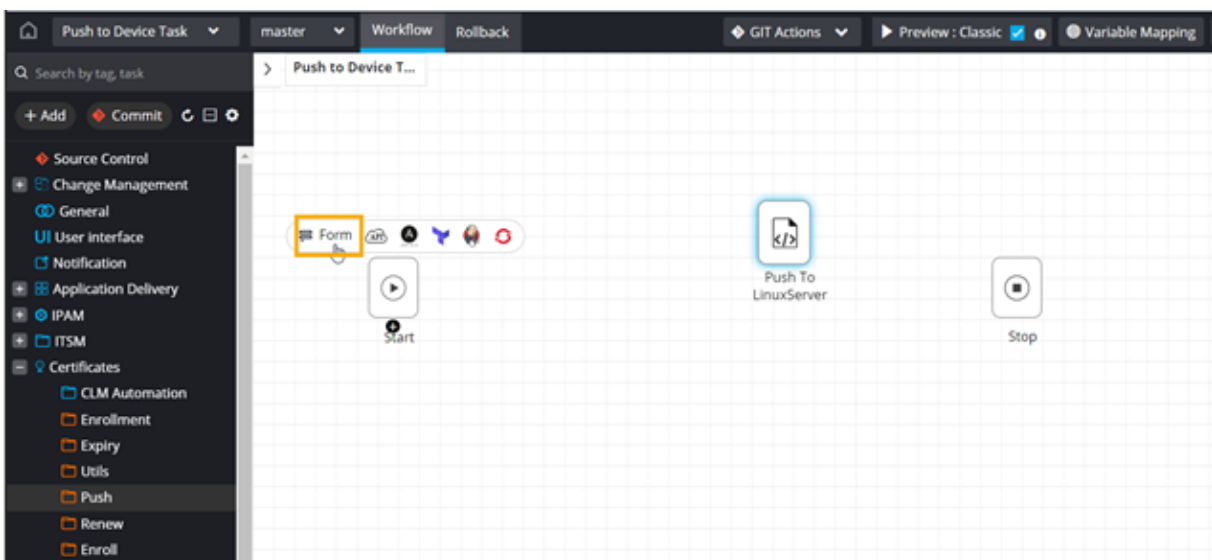


7. From the **Certificates** folder, click **Push**.
The following tasks for pushing certificates are available in the **Push** folder:
 - Push to Apache Server
 - Push to F5 device

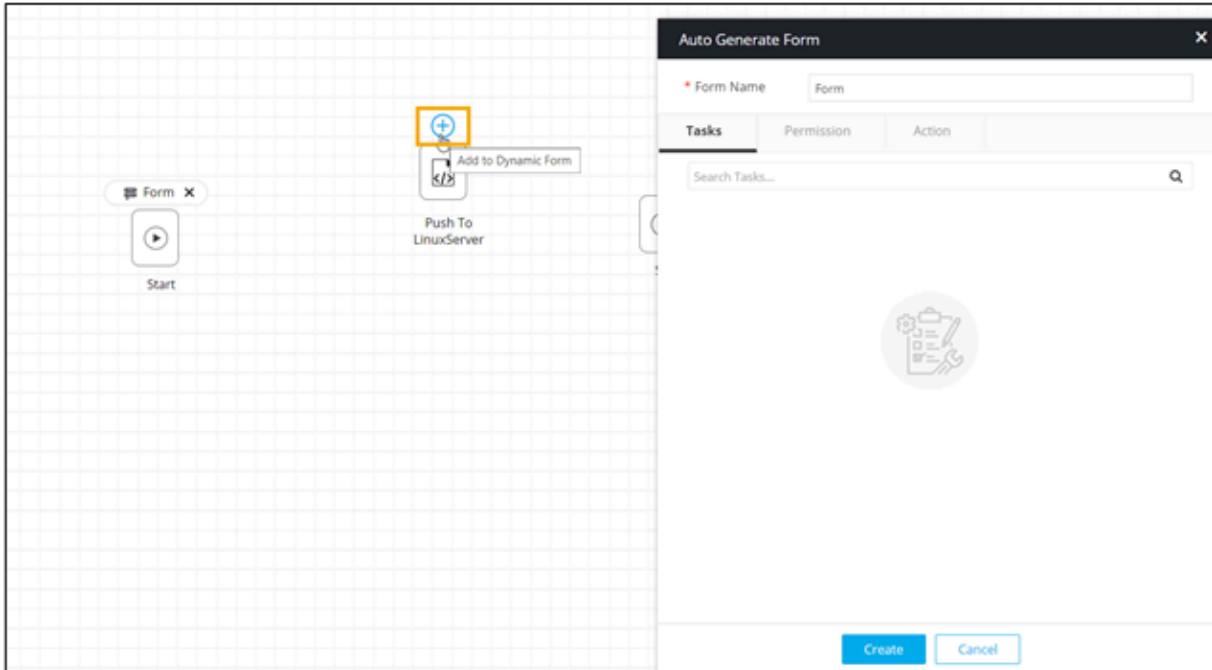
- Push to Citrix Device
 - Push to IIS Server
 - Push to Linux Server
8. From the **Push** folder, drag and drop any of the Push tasks. For example, the **Push to Linux Server** task.



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



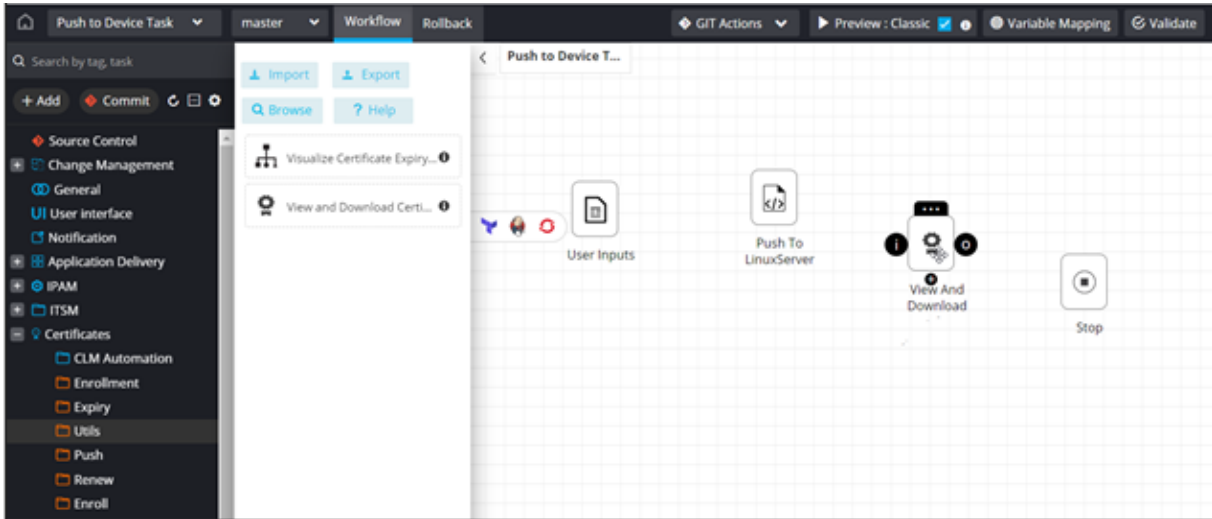
11. Click  above the **Push to LinuxServer** task to auto-populate the form fields.



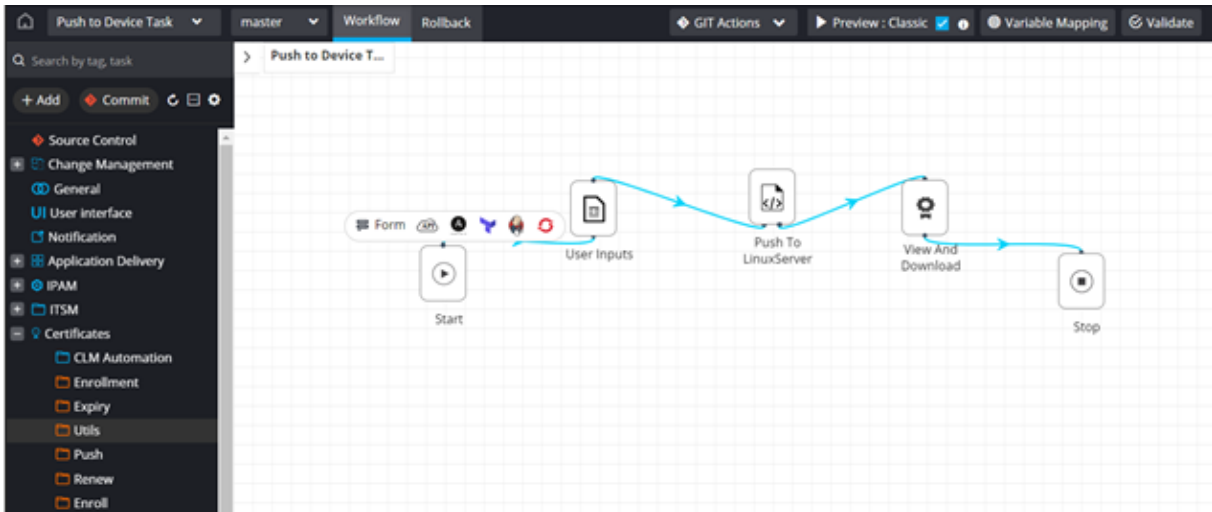
12. Select the fields required in the input form.
13. Provide a **Form Name** and click **Create**.



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.

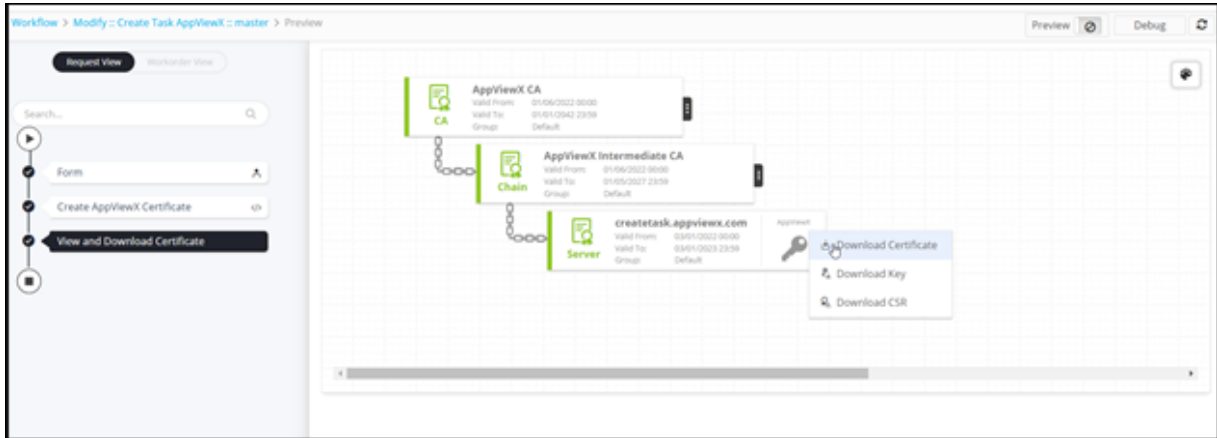
The following table describes the field information in the **User Inputs** form when the **Push to LinuxServer** task is selected:

Field	Description
*Certificate Category	Select the Certificate Profile from the following options: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #00aaff; border-radius: 10px; padding: 10px; background-color: #e6f2ff;">  Note: To retrieve the types of keys that can be availed, click . </div>
*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 .



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



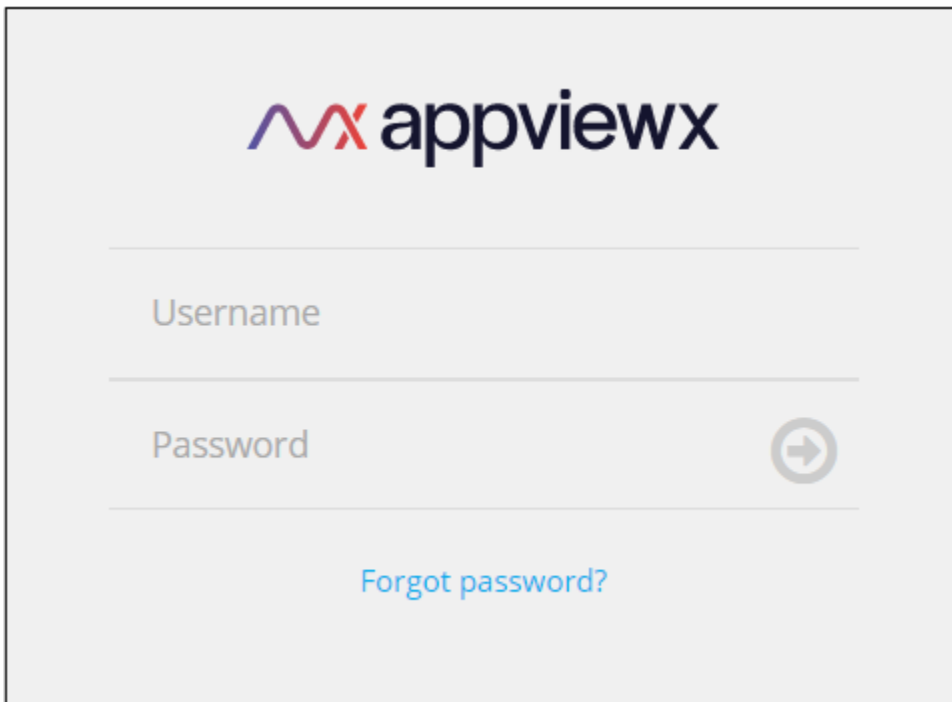
Note: For more information on how to design custom workflows in the Workflow Studio, refer to the Visual Workflow User Guide.


Chapter 9: Designing a Custom Workflow using OOB Tasks

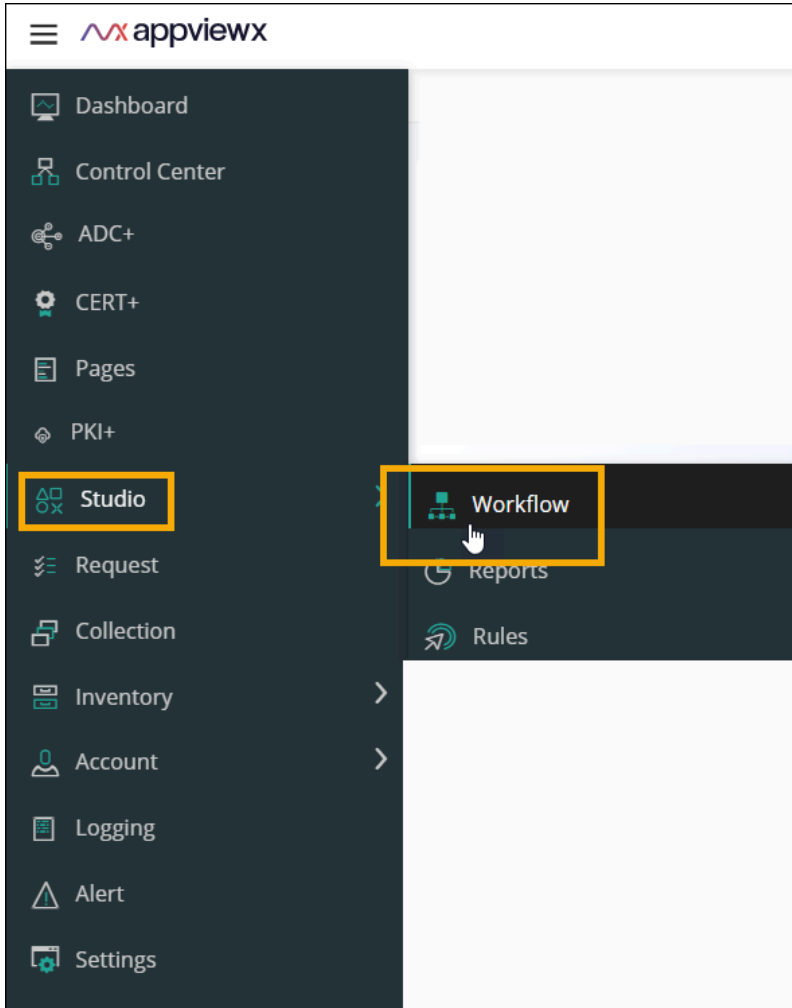
You can use the OOB tasks and subflows available in the Workflow Studio module to build custom workflows for enrolling and renewing certificates. You can also add the OOB Push to Device subflow to push the certificates to a selected device.

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

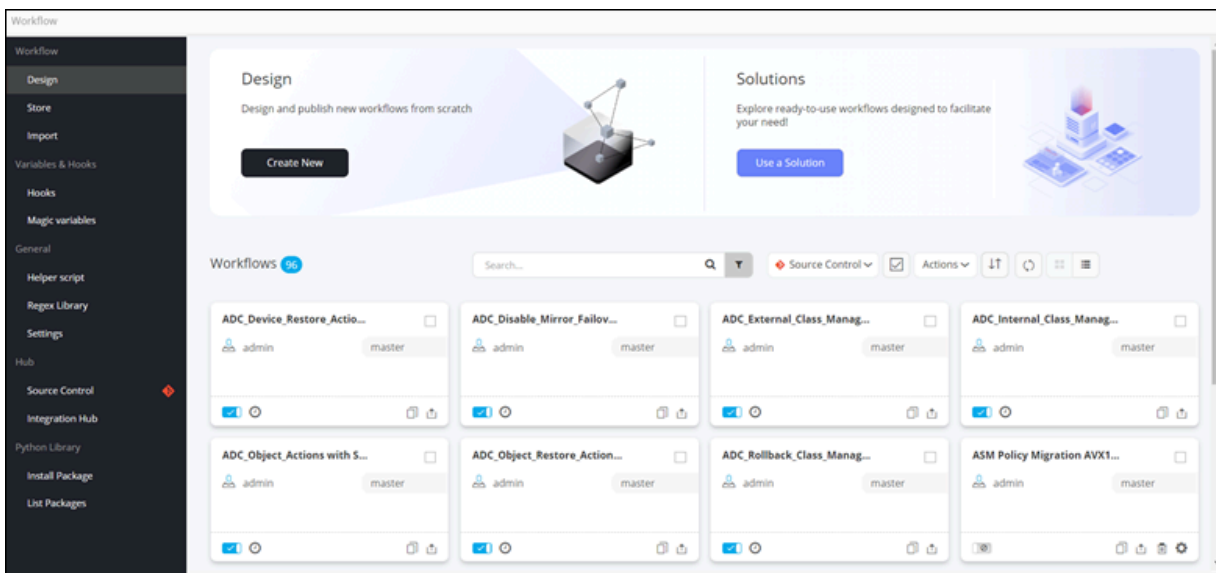
1. Log into AppViewX with valid credentials.



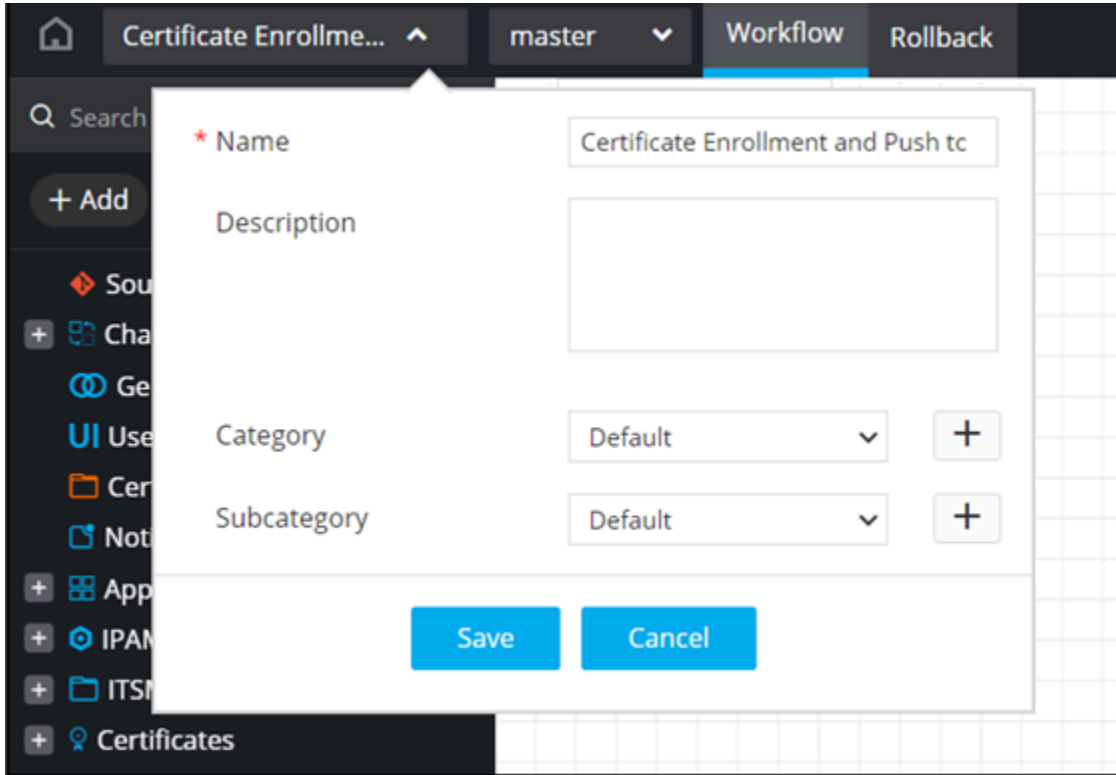
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Studio > Workflow**.



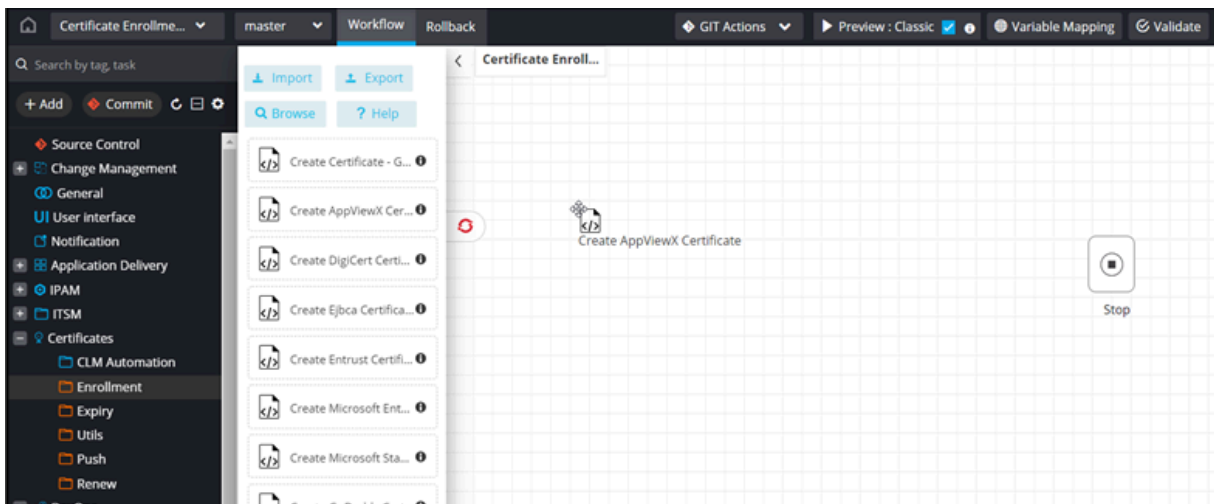
The **Workflow** inventory page is displayed.



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

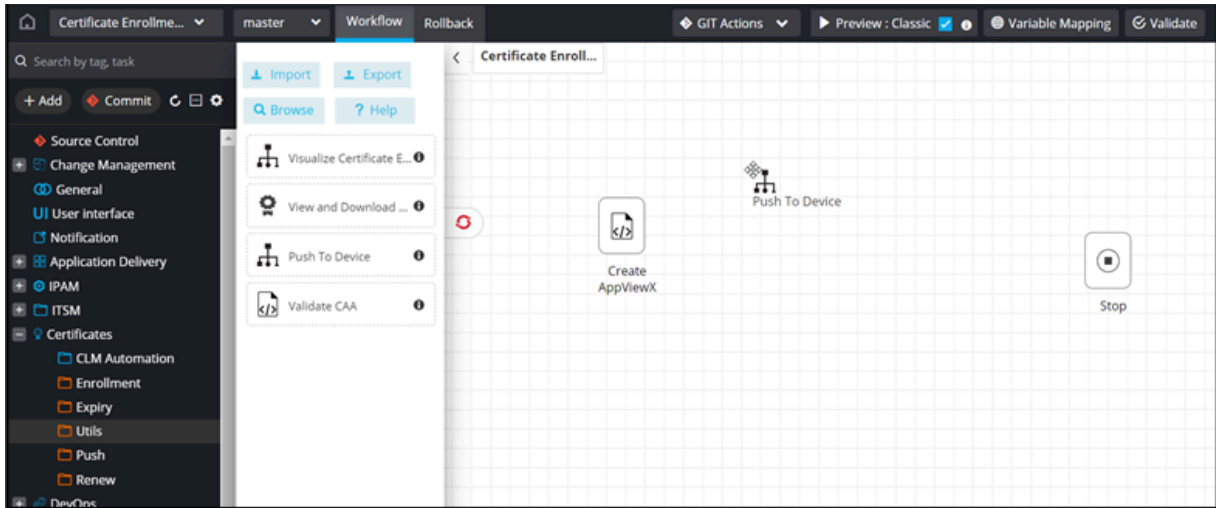


7. To access the OOB workflow tasks, from the left menu, click **Certificates**.
8. Under **Certificates**, from the **Enrollment** folder, drag and drop the required OOB task for enrolling a certificate, for example, the **Create AppViewX Certificate** task.

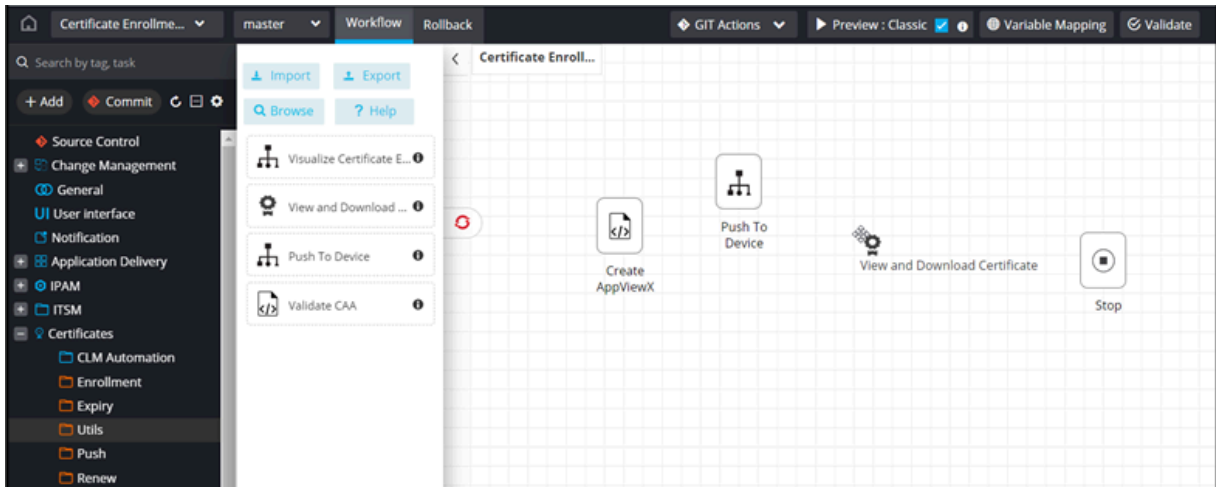


9. Click **Save**.

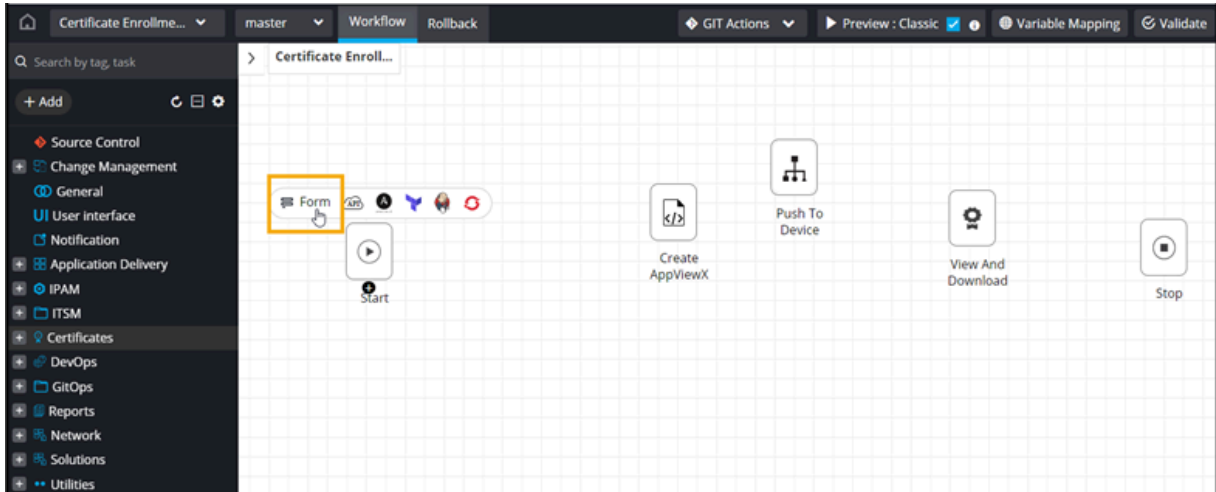
10. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **Push to Device** subflow.



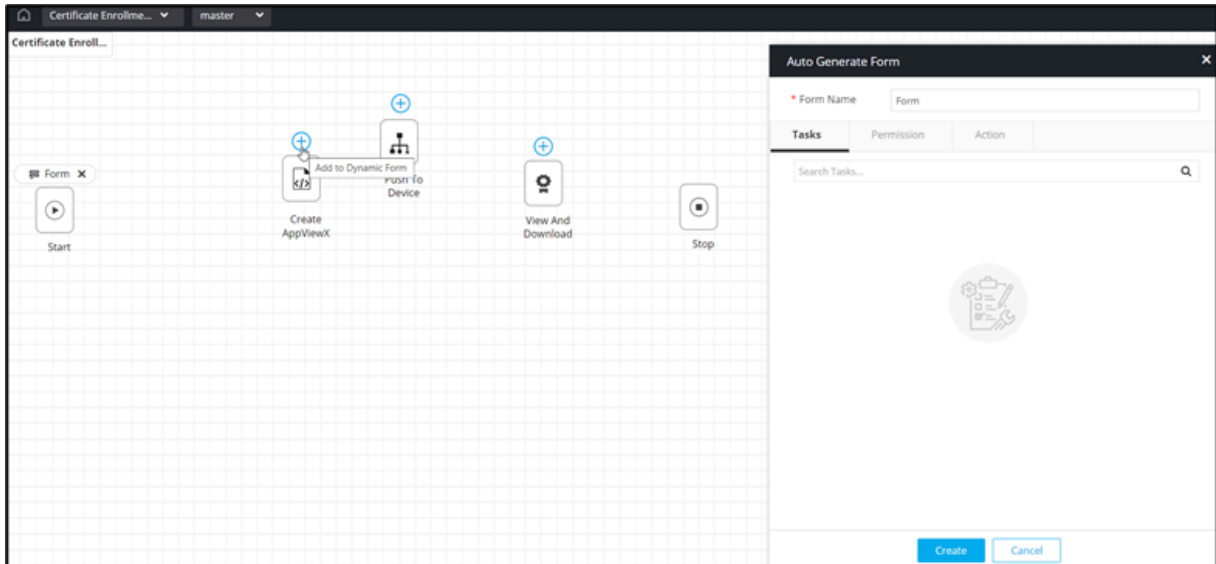
11. Under **Certificates**, from the **Utils** folder, drag and drop the OOB **View and Download Certificate** task.



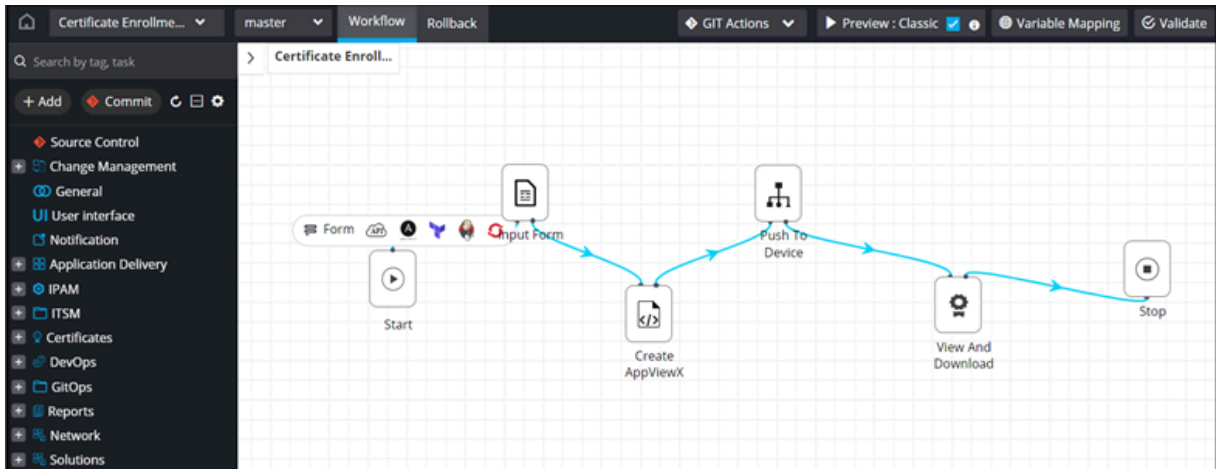
12. To generate a form for this workflow, click **Form** above the **Start** task.



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:

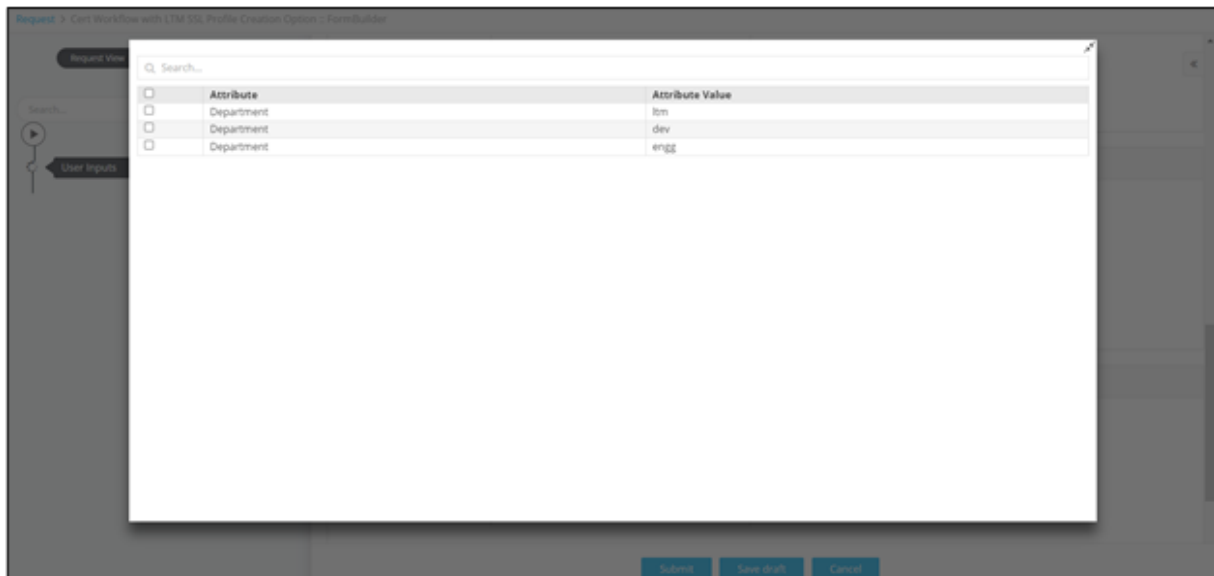
Field	Description
*Certificate Category	<p>Select the Certificate Profile from the following options:</p> <ul style="list-style-type: none"> • Server • Client • Code Signing <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; margin-top: 10px;"> Note: Server is the default selection. </div>

Field	Description
	:
*Certificate Group	Select the Certificate Group from the options available in the dropdown.
*Certificate Authority	<p>Select the Certificate Authority from the options available in the dropdown. The following CAs are supported:</p> <ul style="list-style-type: none"> • DigiCert • Entrust • EJBCA • Microsoft Enterprise • AppViewX <p> Note: This field is populated based on the Certificate Group selected.</p>
*CA Account	<p>Select the CA Account from the options available in the dropdown.</p> <p> Note: This field is populated based on the Certificate Authority selected.</p>
*Division	<p>Select the Division from the options available in the dropdown.</p> <p> Note: This field is displayed only when DigiCert is selected as the CA.</p>
Certificate Type	Select the Certificate Type from the options available in the dropdown.
*Auto Renewal	<p>Select the required radio button to enable/disable Auto Renewal.</p> <p> Note: Default selection is set to Off.</p>
Renew Before (Days)	<p>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.</p> <p> Note: This field is displayed only when the Auto Renewal field is enabled.</p>
Description	Enter a description for the certificate to be created.

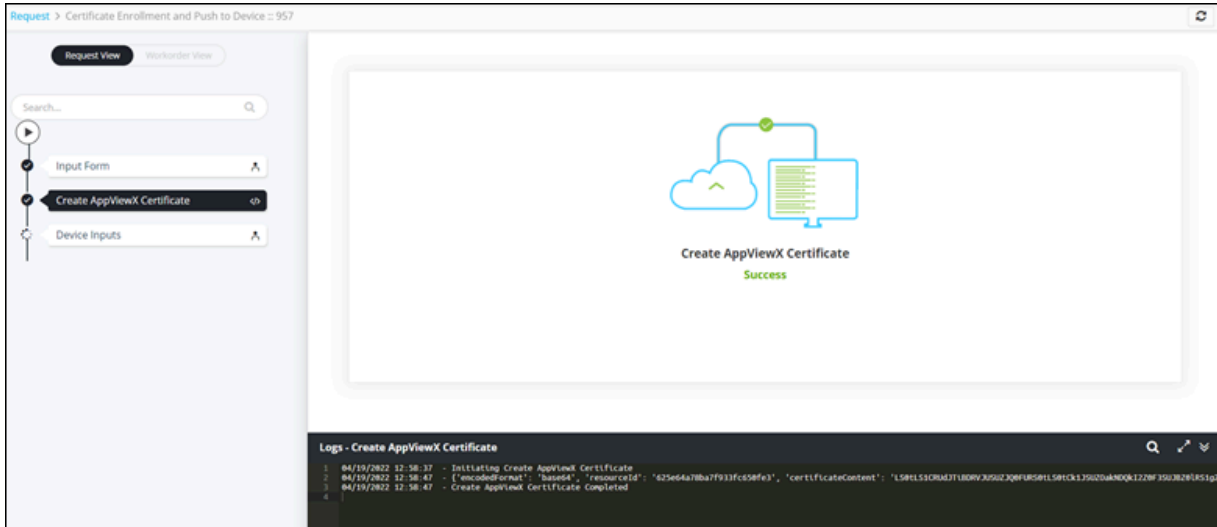
Field	Description
*Common Name	Enter the Fully Qualified Domain Name (FQDN) of the server for which certificate is requested.
Subject Alternative Name	Select the SAN as either: <ul style="list-style-type: none"> • DNS • IP Address
DNS	Enter a valid DNS if you select the DNS option in the SAN field.
IP 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: <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: This field will be populated based on the selected Key Type. </div>

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.	

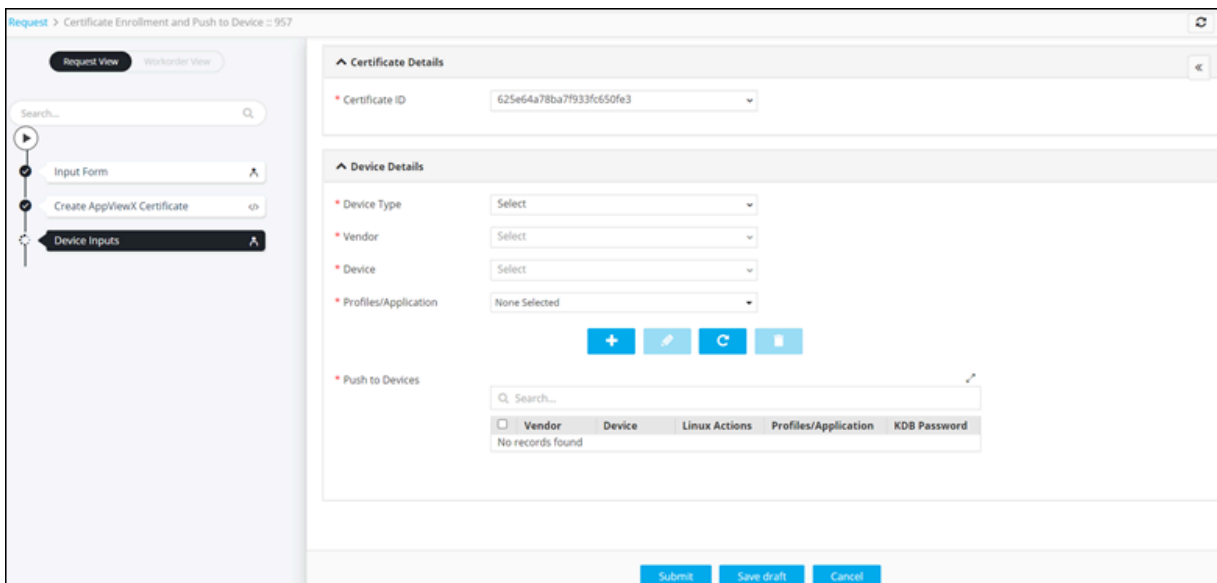
17. To add this attribute to the **Certificate Attributes** grid, click .
18. To edit the value of a particular attribute, select the attribute in the grid and click .
19. Enter the new value for the attribute in the **Value** field and click  again to update the value.
20. To delete a certificate attribute,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

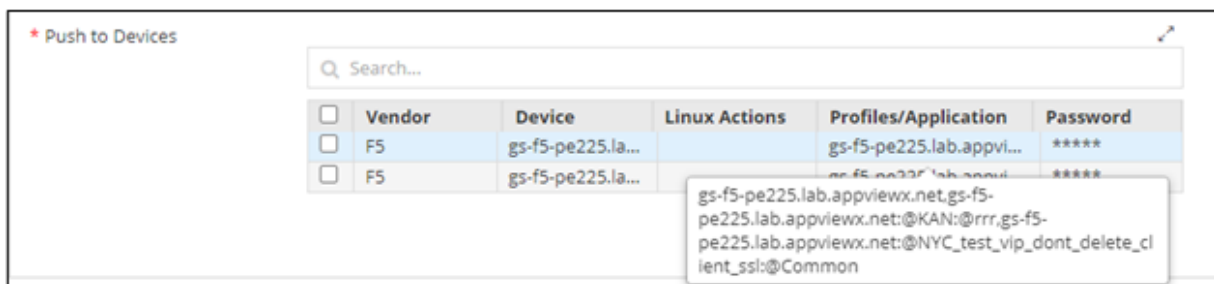
Field	Description
* Device Type	Select the Device Type from the options available in the dropdown.
* Vendor	Select the Vendor from the options available in the dropdown. <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 5px; display: inline-block;"> Note: The vendor list is populated based on the Device Type selected. </div>
* 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.	

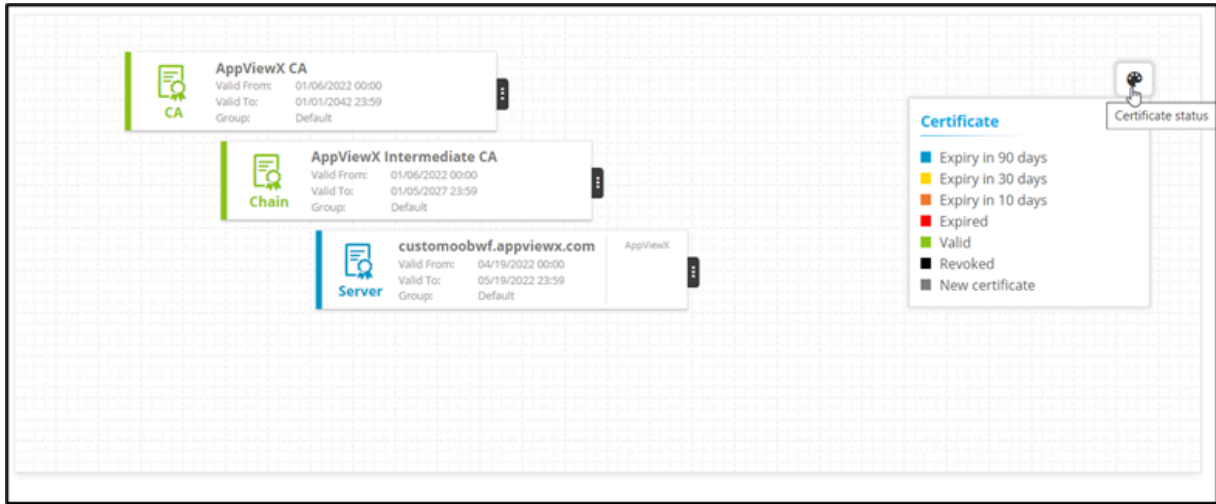
25. To add the selected profile/application to the grid, click .

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.



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.

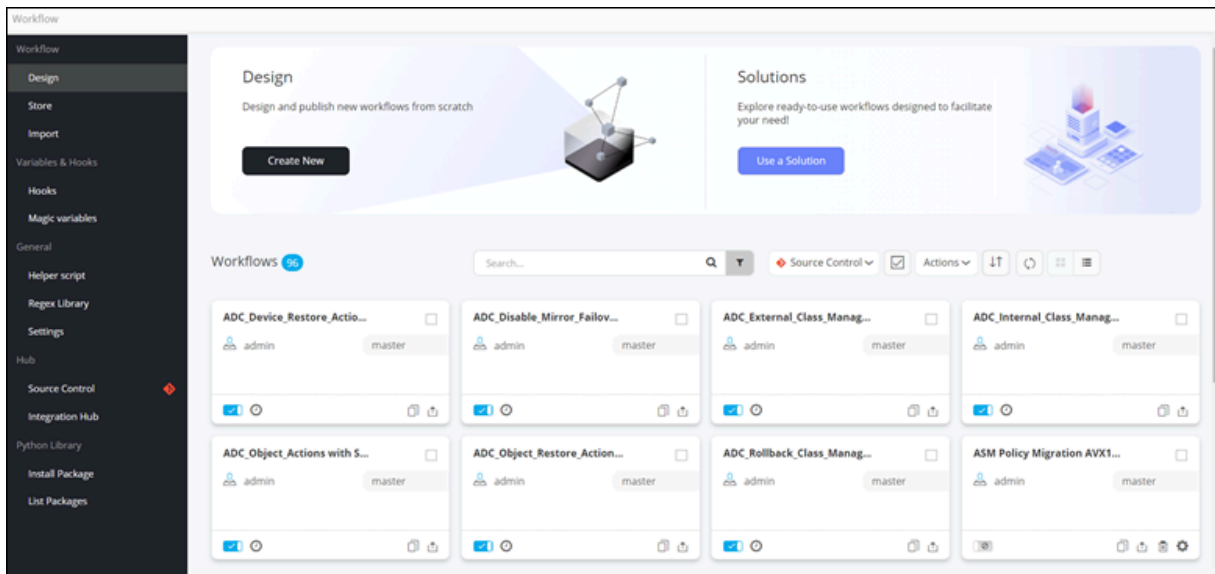
Chapter 11: Customizing an OOB Workflow

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

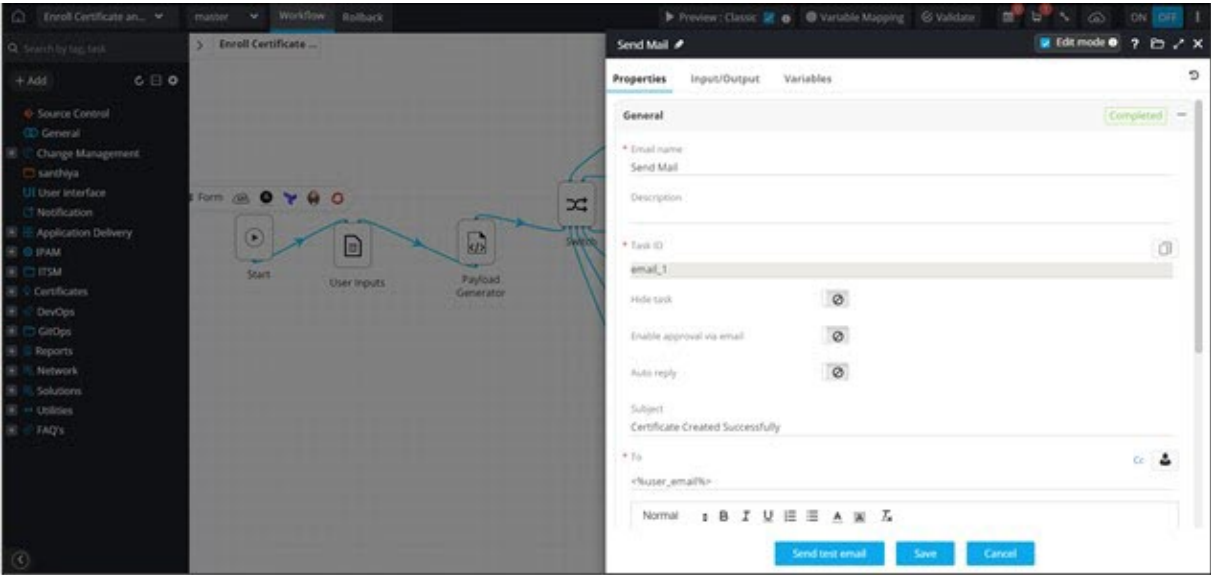
To customize a workflow:


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

The **Workflow Inventory** page is displayed.

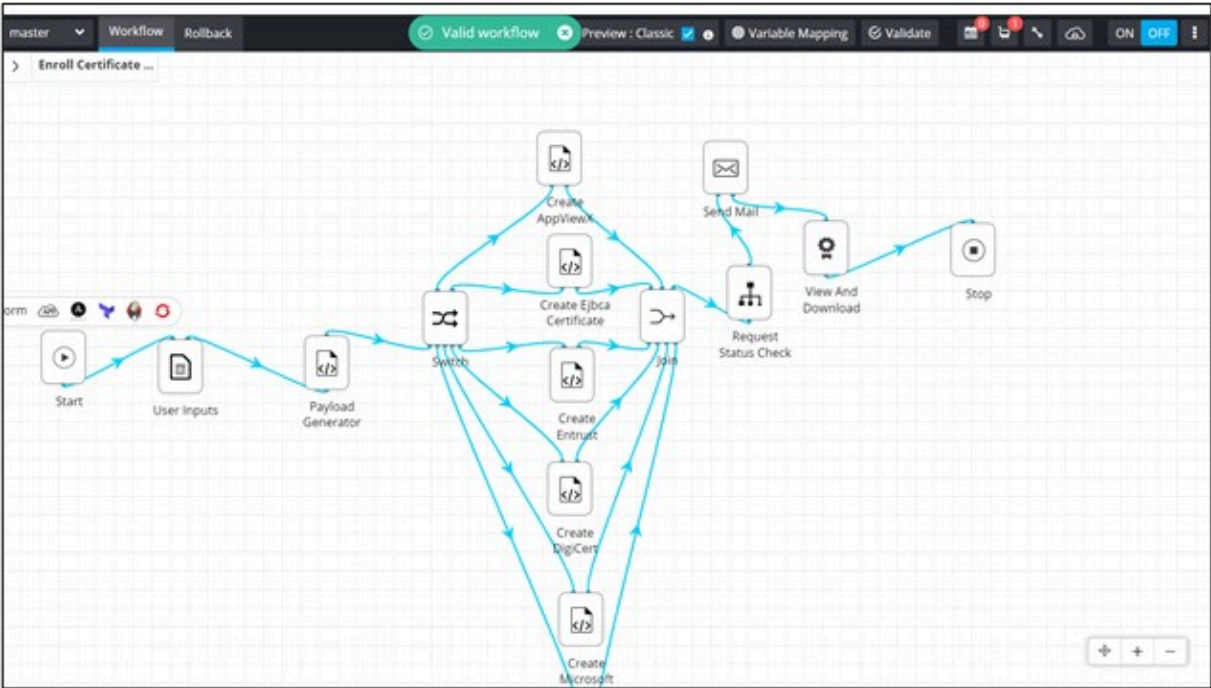



2. Search for the workflow by typing the keyword in the search bar.
3. Disable the workflow by turning off the toggle on the workflow card.
4. Click on the workflow to open it in the design space.
5. Modify the required tasks.



 **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.