



CERT+ Automation Workflows User Guide

Version: 2021.1.0

Copyright AppViewX, Inc.

Copyright © 2021 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.....	4
Revision History.....	4
About this Guide.....	4
Audience.....	4
Text Conventions.....	4
Chapter 1. Prerequisites	5
Chapter 2. Role-Based Access Control.....	6
Chapter 3. Accessing CERT+ Automation Workflows.....	7
Chapter 4. Certificate Expiry Workflows.....	11
Overview.....	11
Certificate Expiry Notification based on Certificate Attributes.....	11
Certificate Expiry Notification - Cert Group Hierarchy.....	16
Certificate Expiry Notification - Days.....	20
Certificate Expiry Notification - Devices Servers.....	24
Certificate Expiry Notification.....	30
Update Certificate Attributes.....	34
Certificate Expiry Notification with JIRA.....	40
Certificate Expiry Notification with ServiceNow.....	45
Orphan Certificates Report.....	49
Chapter 5. Certificate Expiry Notification task.....	55
Chapter 6. Scheduling an OOB workflow.....	65

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2021.1.0	September 2021

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

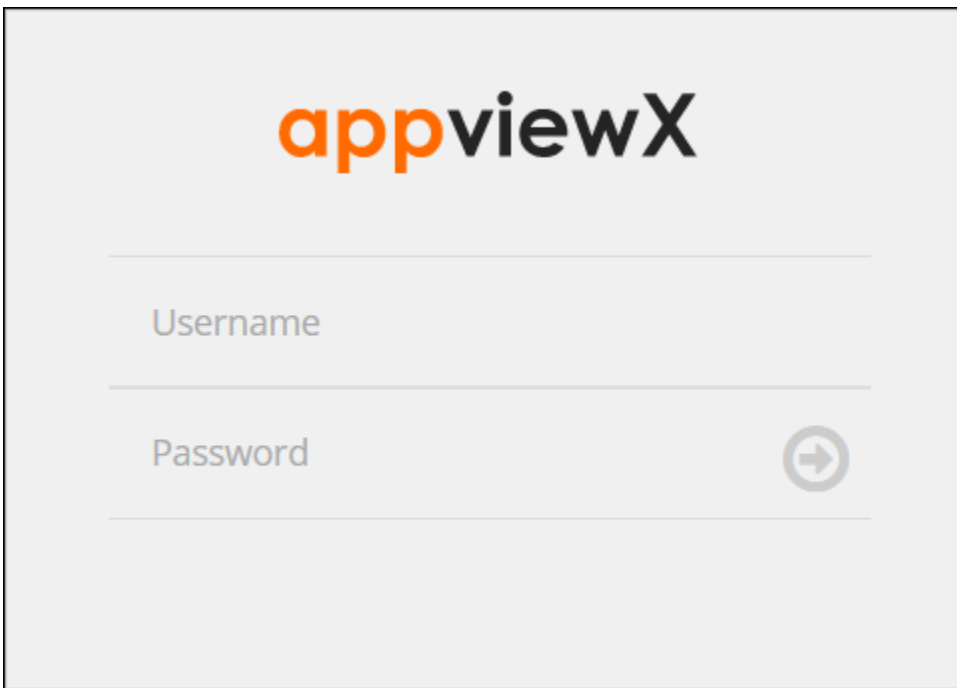
With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to [this link](#) and find out more about RBAC.


Chapter 3: Accessing CERT+ Automation Workflows

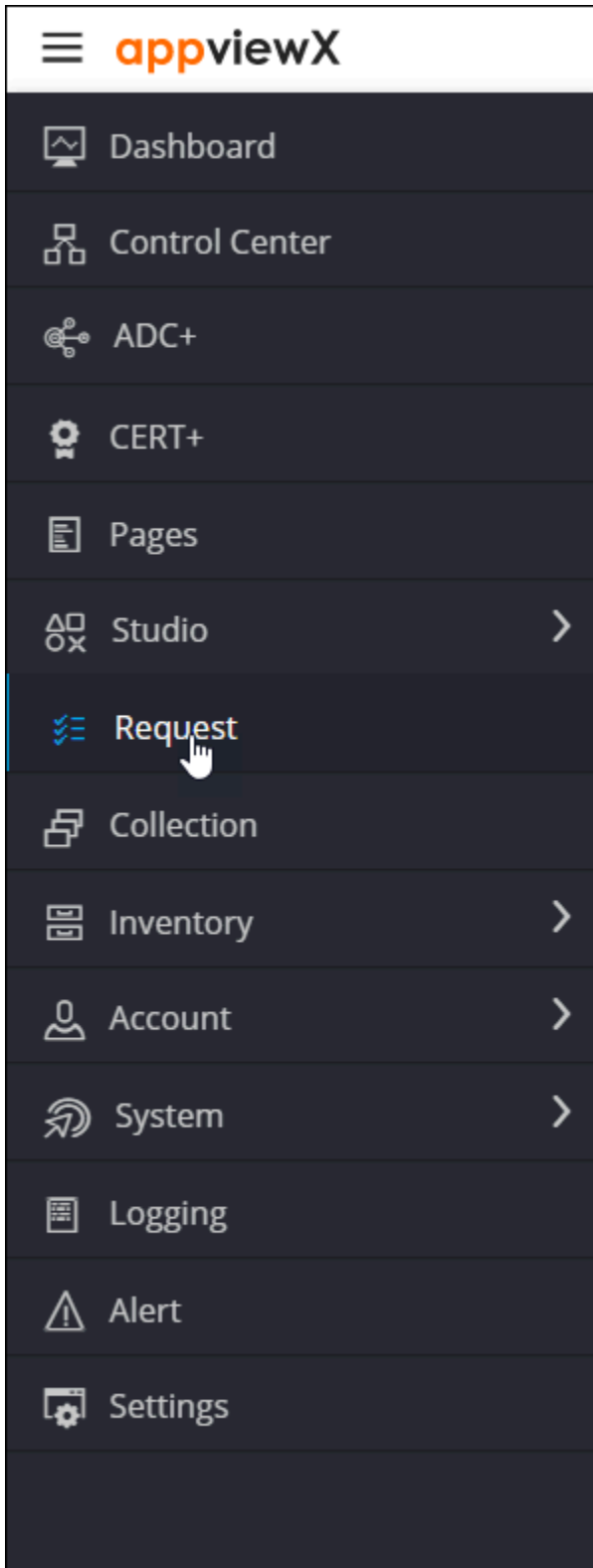
The CERT+ Automation workflows are available on the Workflow **Catalog** page.

To view these workflows:

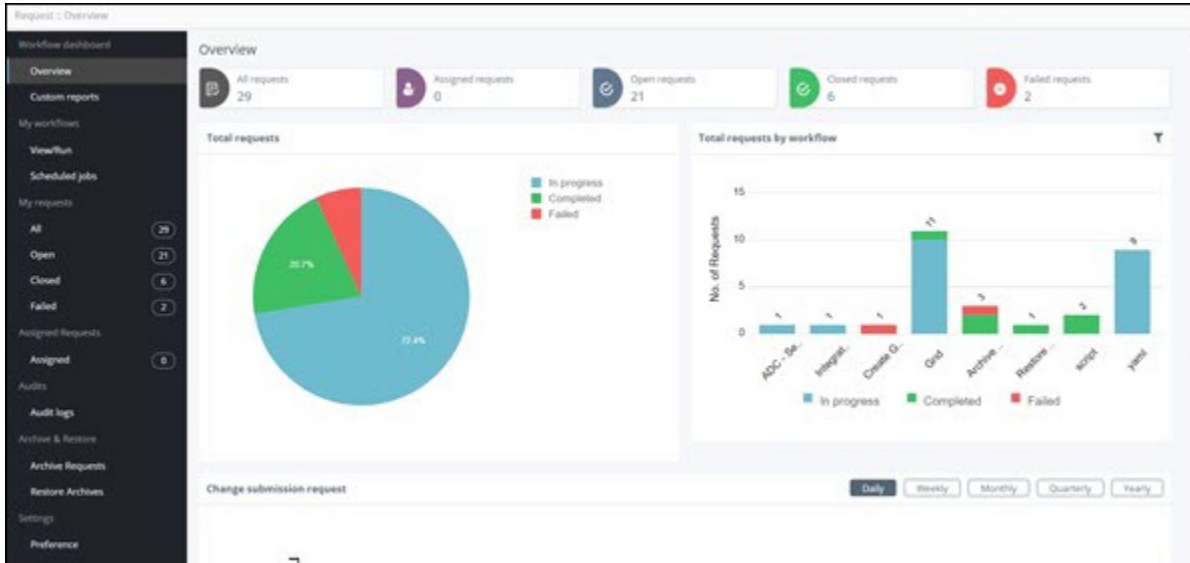
1. Log into AppViewX with valid credentials.

A screenshot of the AppViewX login interface. At the top center is the 'appviewX' logo, with 'app' in orange and 'viewX' in black. Below the logo are two input fields: 'Username' and 'Password'. The 'Password' field includes a circular icon with a right-pointing arrow on its right side. The entire form is set against a light gray background.

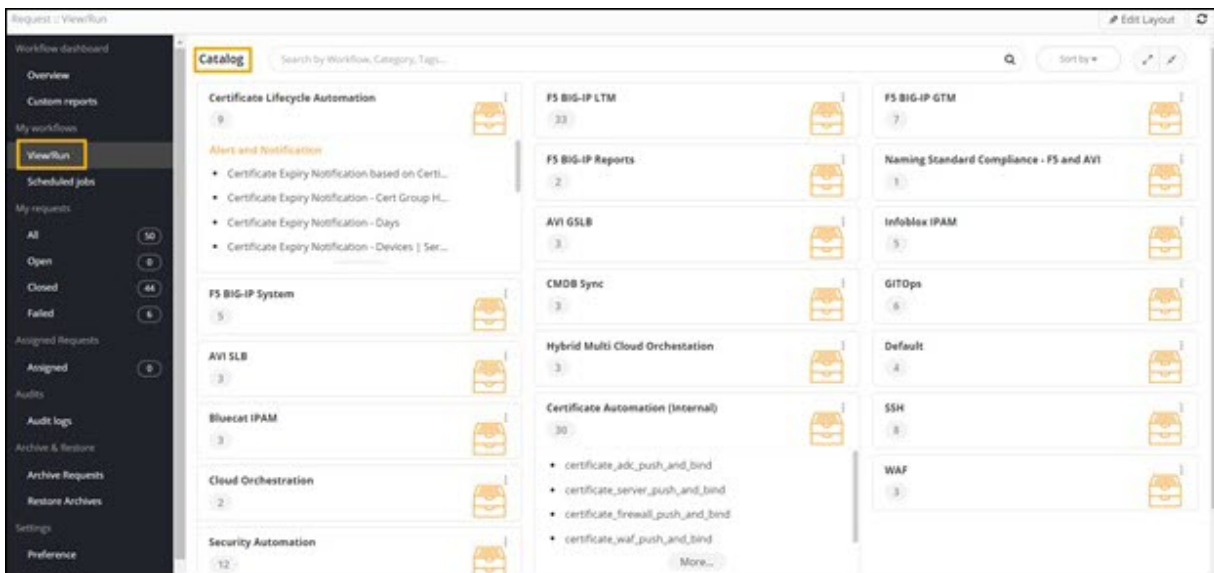
2. To access the navigation pane, hover the mouse over  .
3. From the menu displayed, click **Request**.



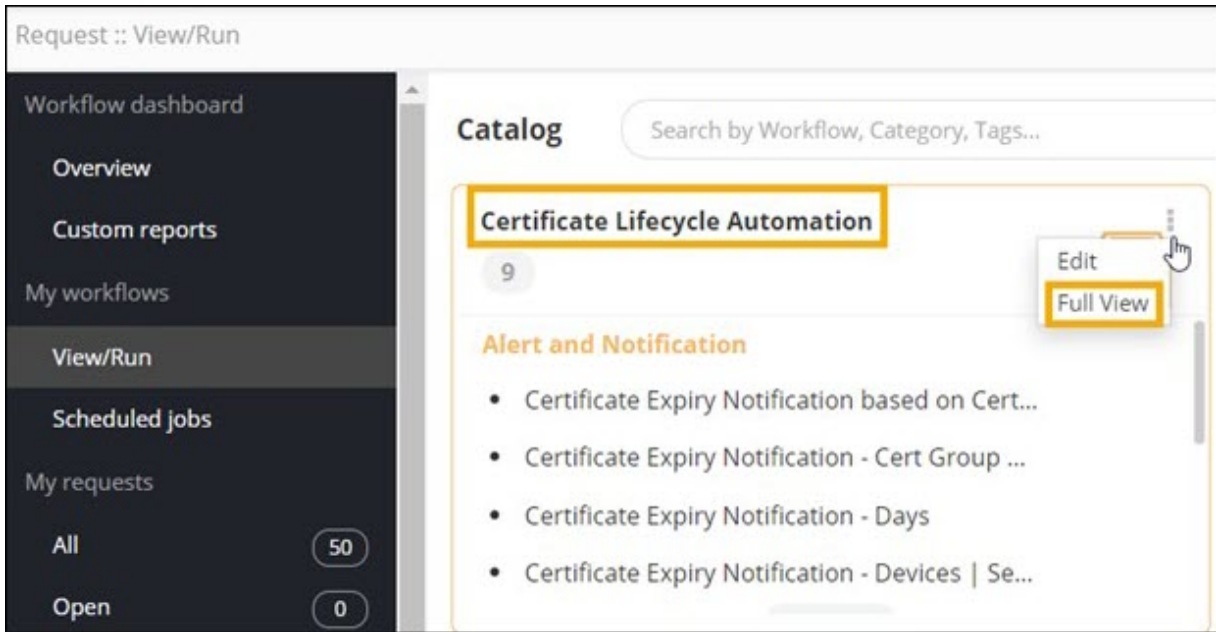
The Workflow **Request** page is displayed, with the **Overview** section open by default.



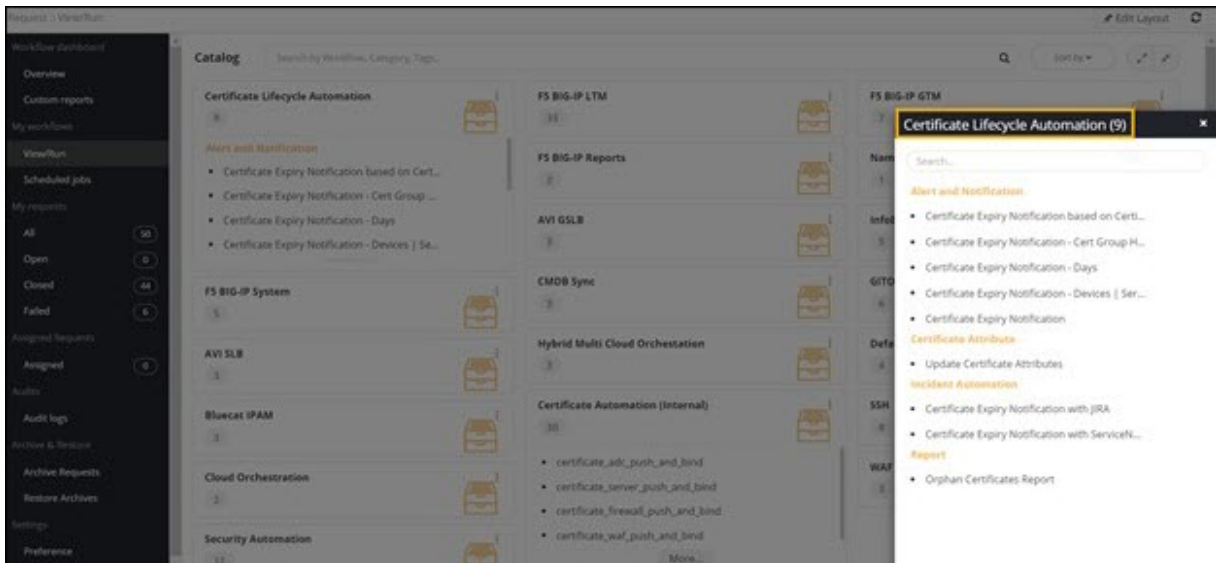
- On the Workflow **Request** page, from the navigation menu on the left, select **View/RUN**. The workflow **Catalog** page is displayed.



- 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: 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

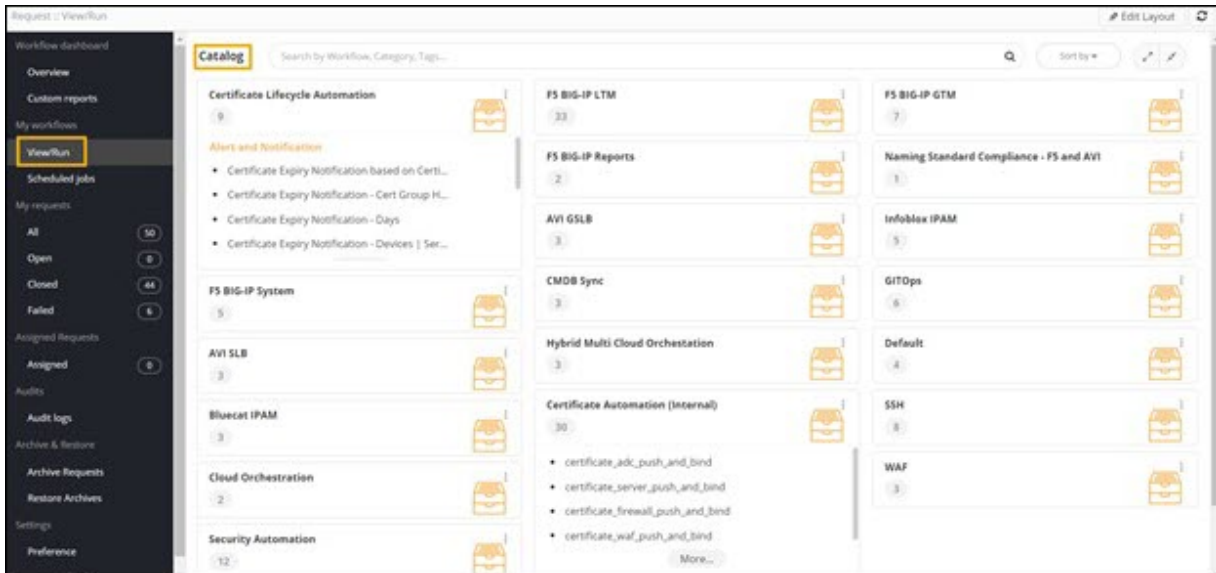
This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. It also enables you to create tickets for expiring certificates on Jira/ServiceNow.



Certificate Expiry Notification based on Certificate Attributes

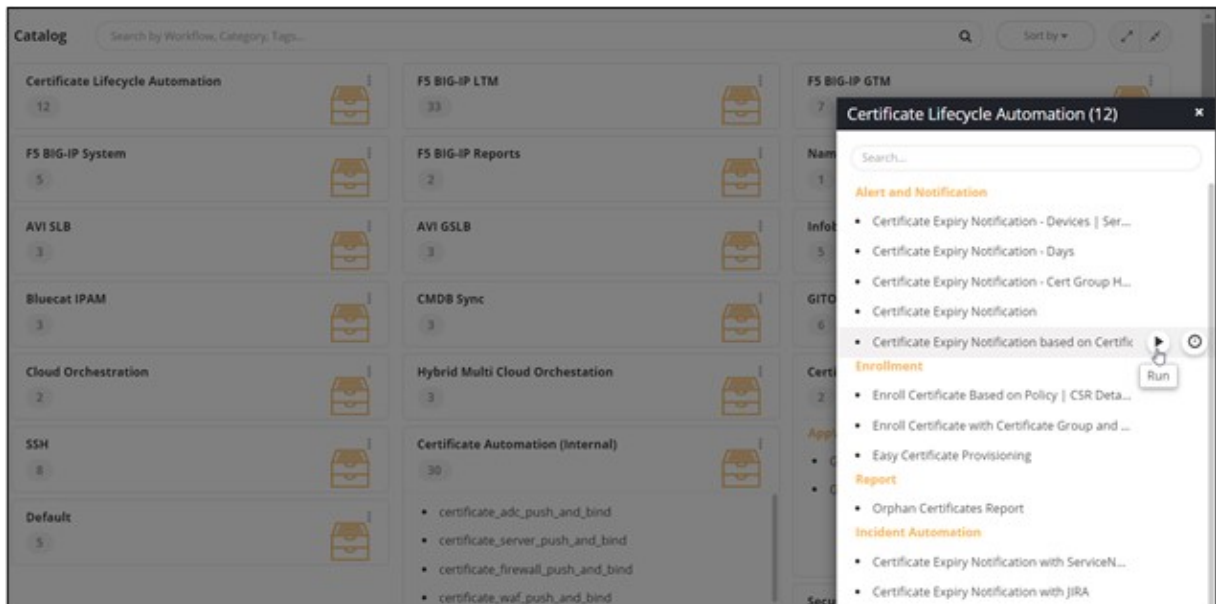
This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.


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.

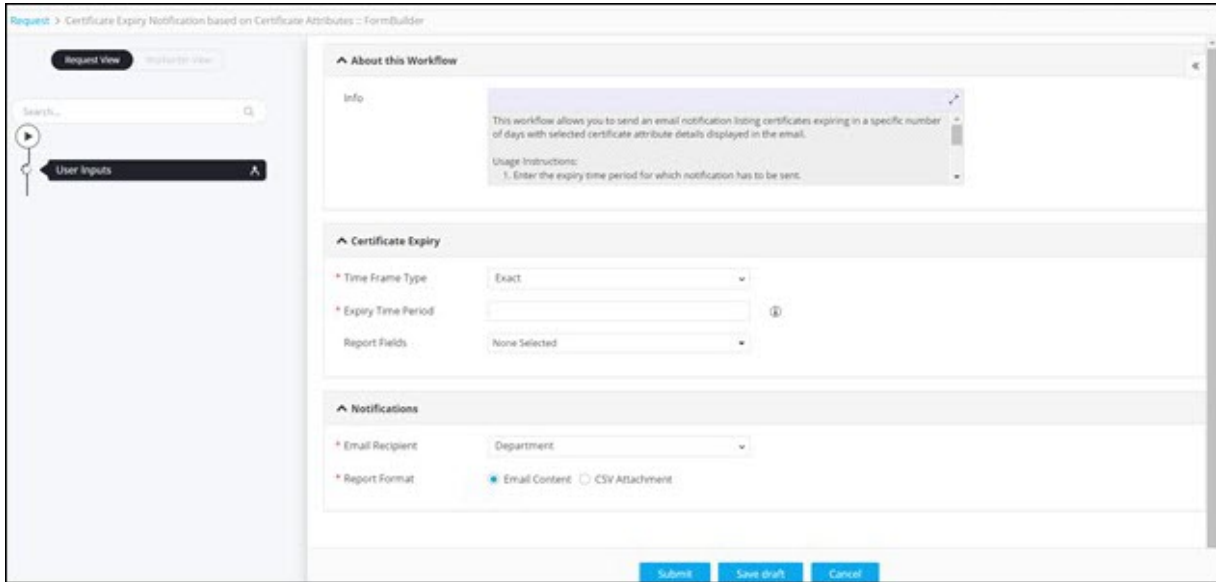


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

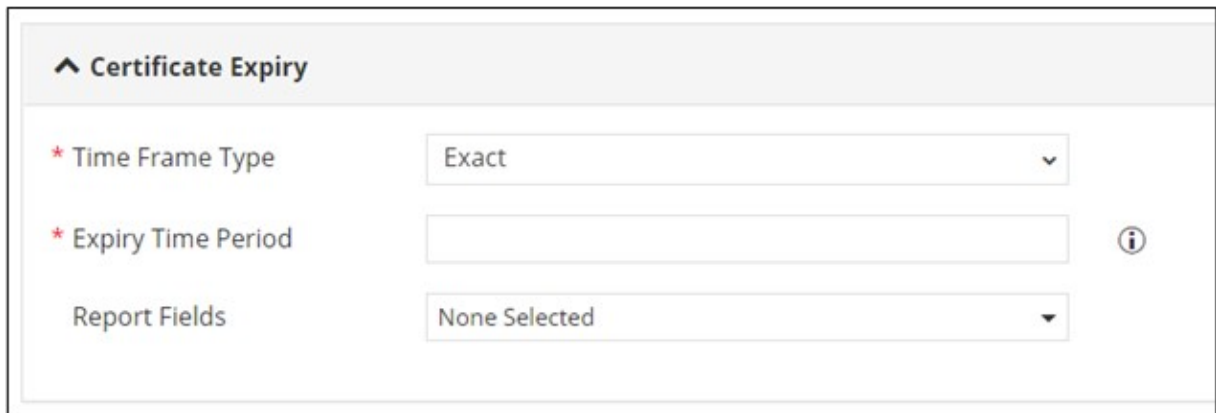


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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. • 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.

The screenshot shows a 'Notifications' section with the following fields:

- * Email Recipient**: A dropdown menu with 'Department' selected.
- * Report Format**: Two radio buttons, 'Email Content' (selected) and 'CSV Attachment'.

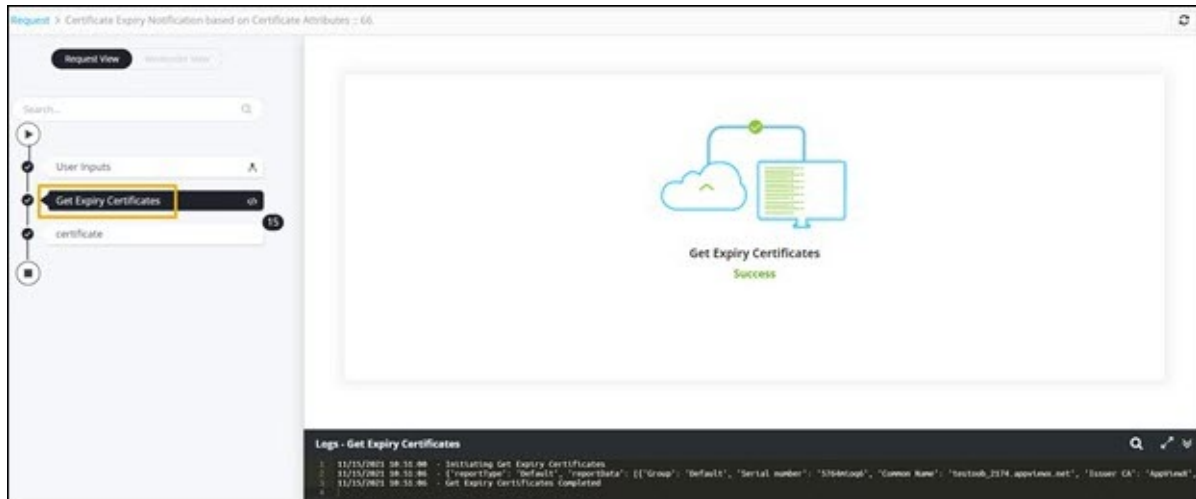
The following table describes the fields under the **Notifications** section:

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> <ul style="list-style-type: none"> • CSV Attachment - The report will be sent as a separate attachment in CSV format.

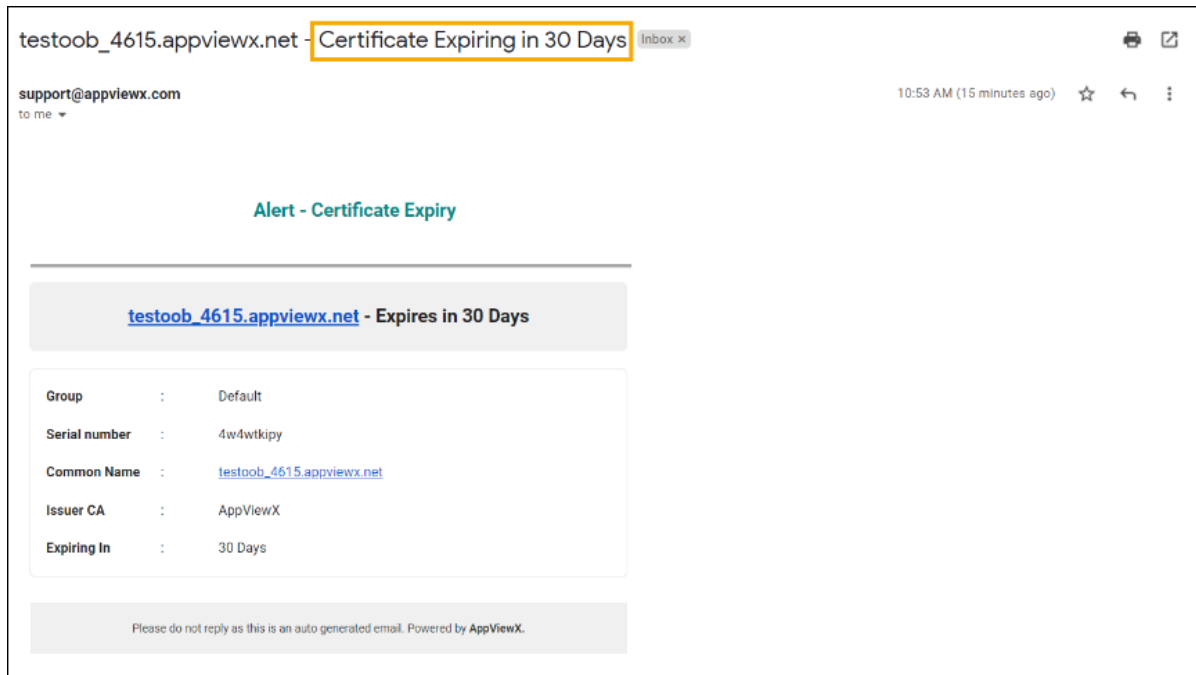
Field	Description
	 Note: Email Content is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

- **Get Expiry Certificates** task completed.



- Email notification received individually for expiring certificates.



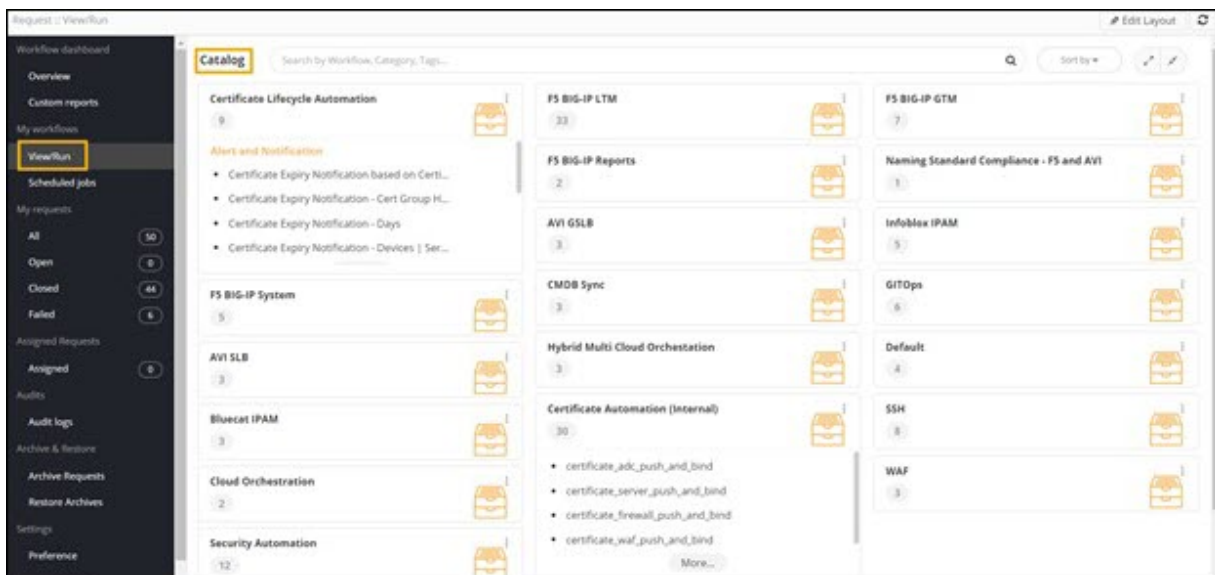
Certificate Expiry Notification - Cert Group Hierarchy



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

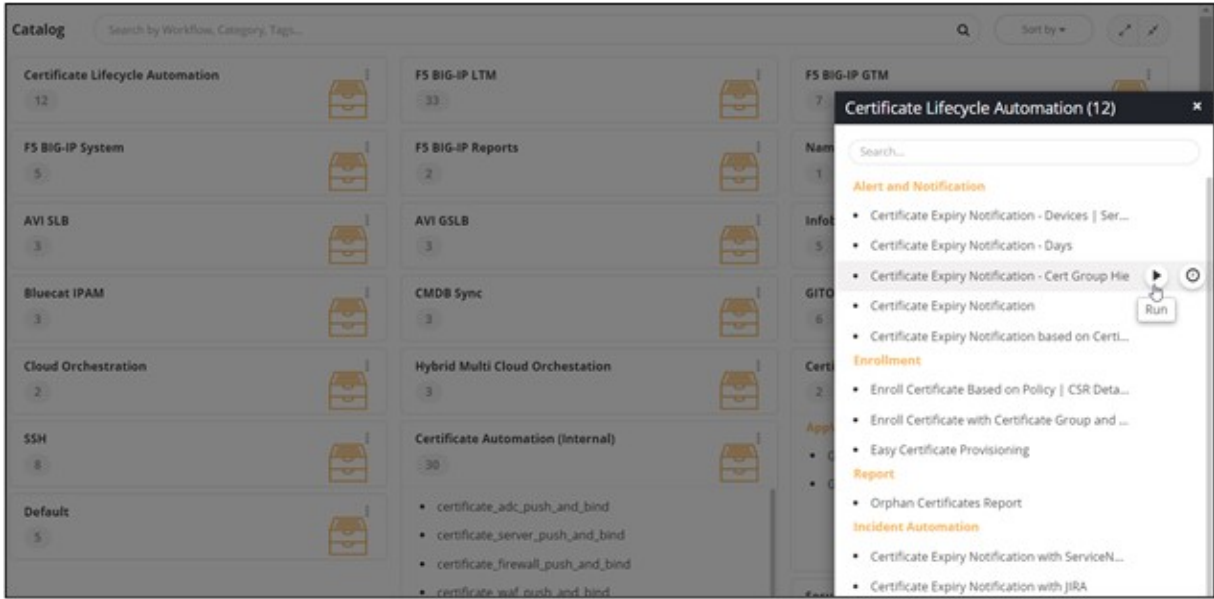
To trigger this workflow:

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

The workflow **Catalog** page is displayed.

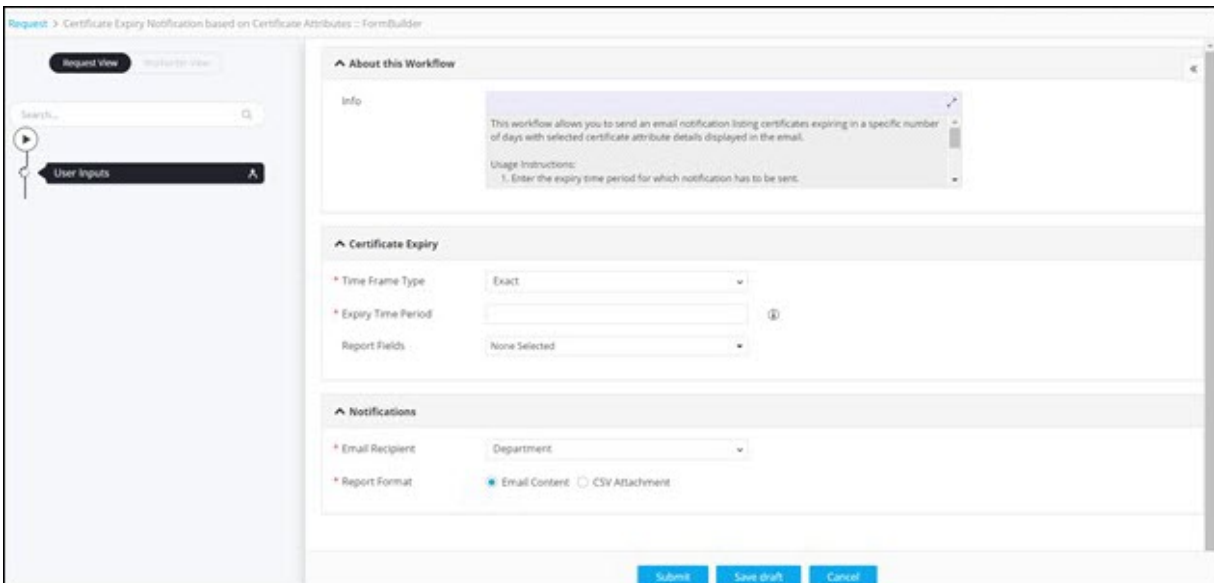


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click  .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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



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.



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

^ Certificate Expiry

* Time Frame Type

* Expiry Time Period ⓘ

Report Fields

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 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

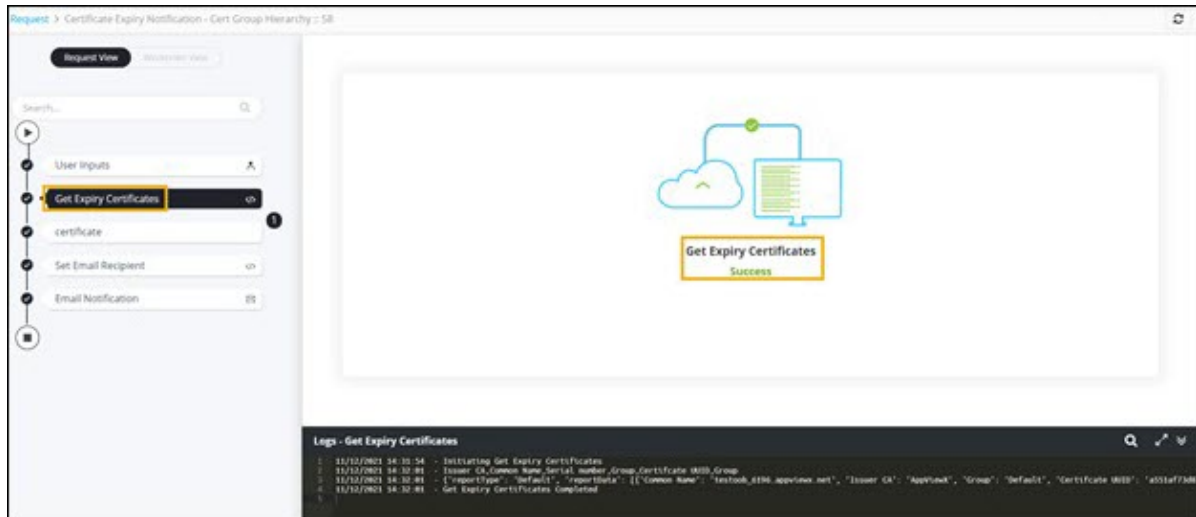
* Report Format Email Content CSV Attachment

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

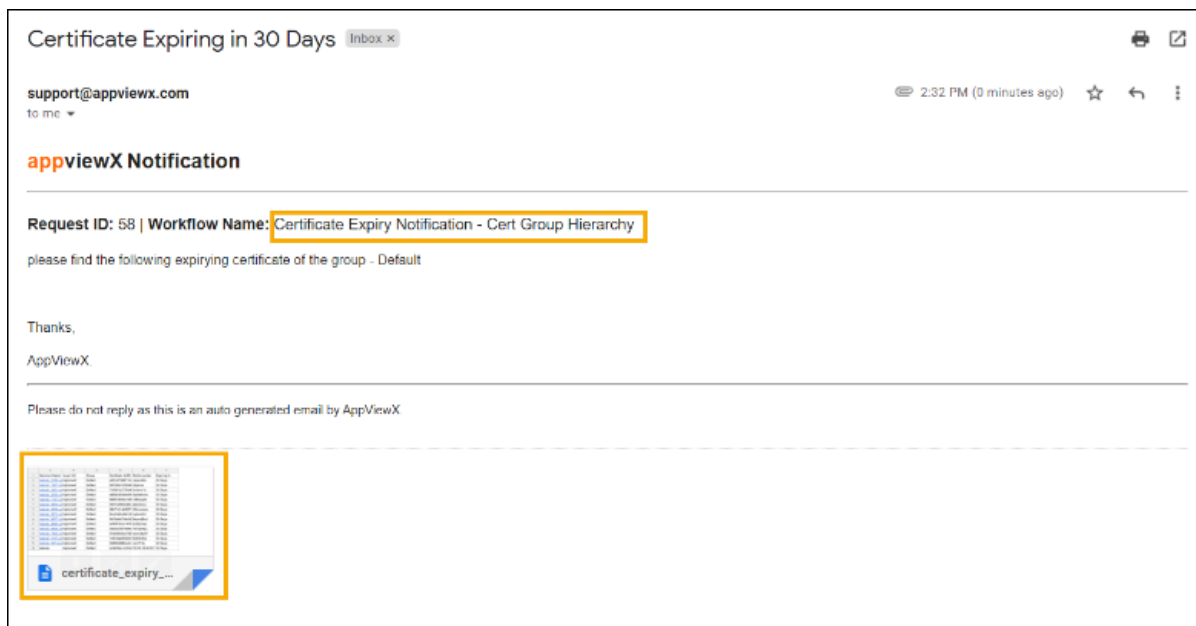
Field	Description
* Notify Parent Group	<p>Select On if a notification has to be sent to the parent group of the certificate group.</p> <p>Select Off if a notification is not required to be sent to the parent group of the certificate group.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: On is the default selection. </div>
* 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 #add8e6; 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.

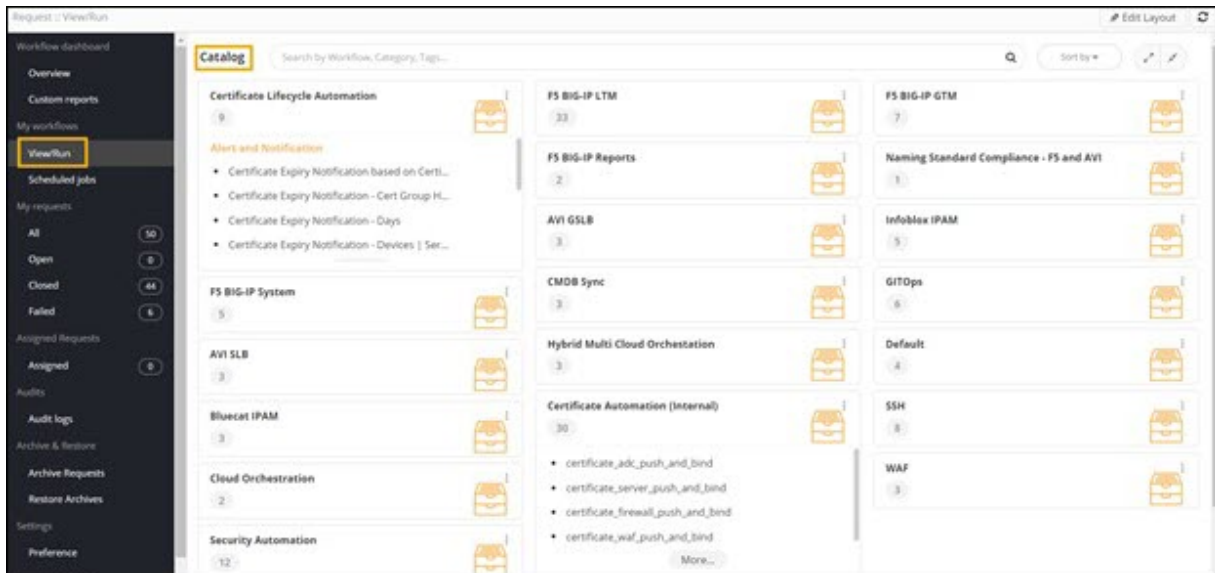




Certificate Expiry Notification - Days

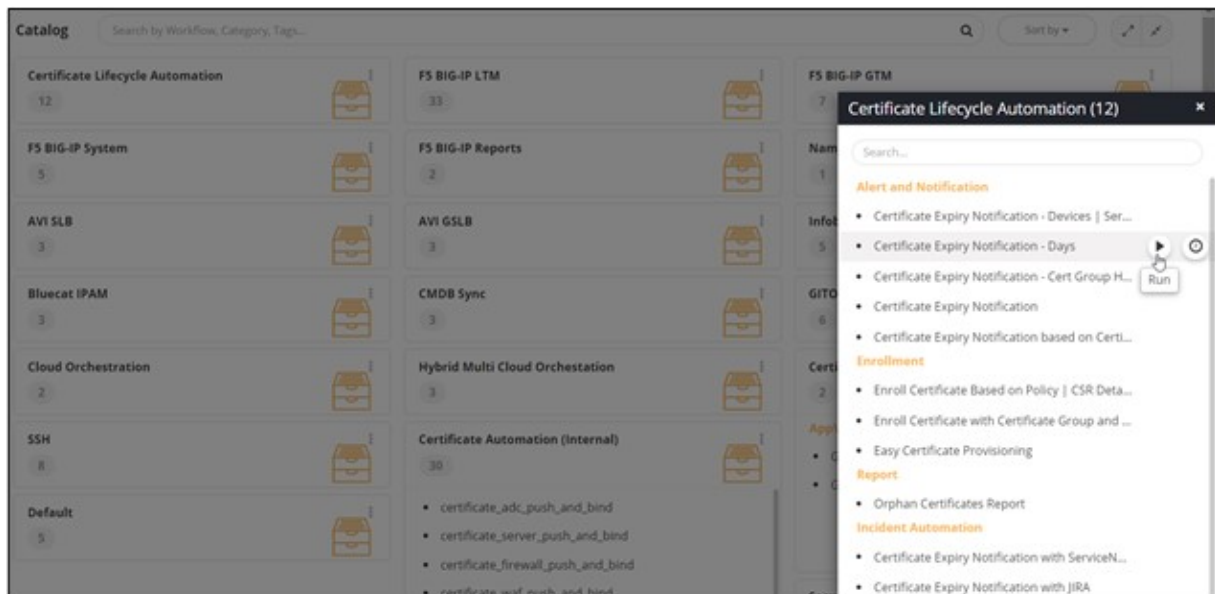
This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.

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.

Field	Description
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

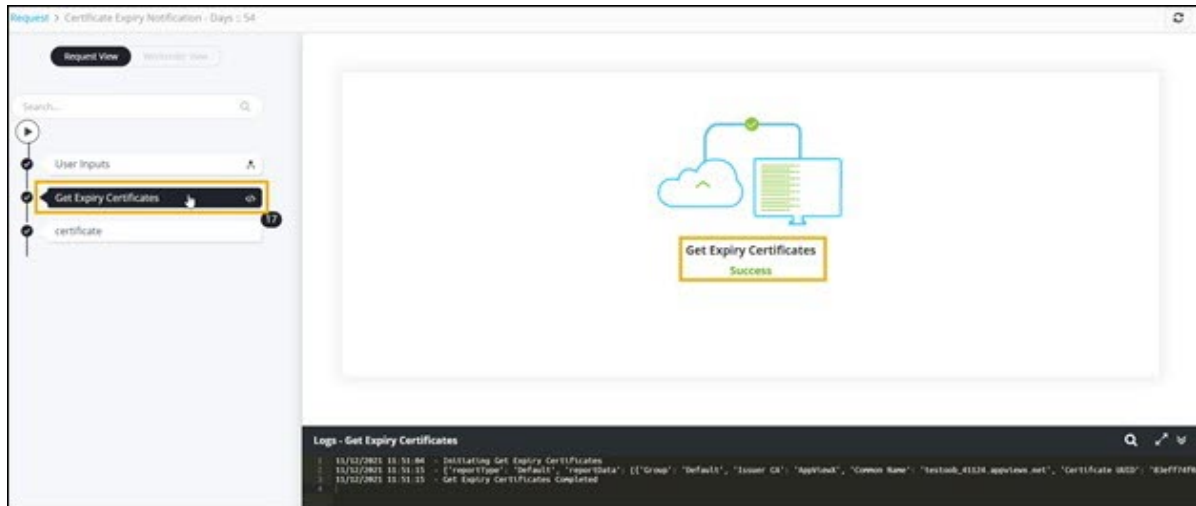
* Report Format Email Content CSV Attachment

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

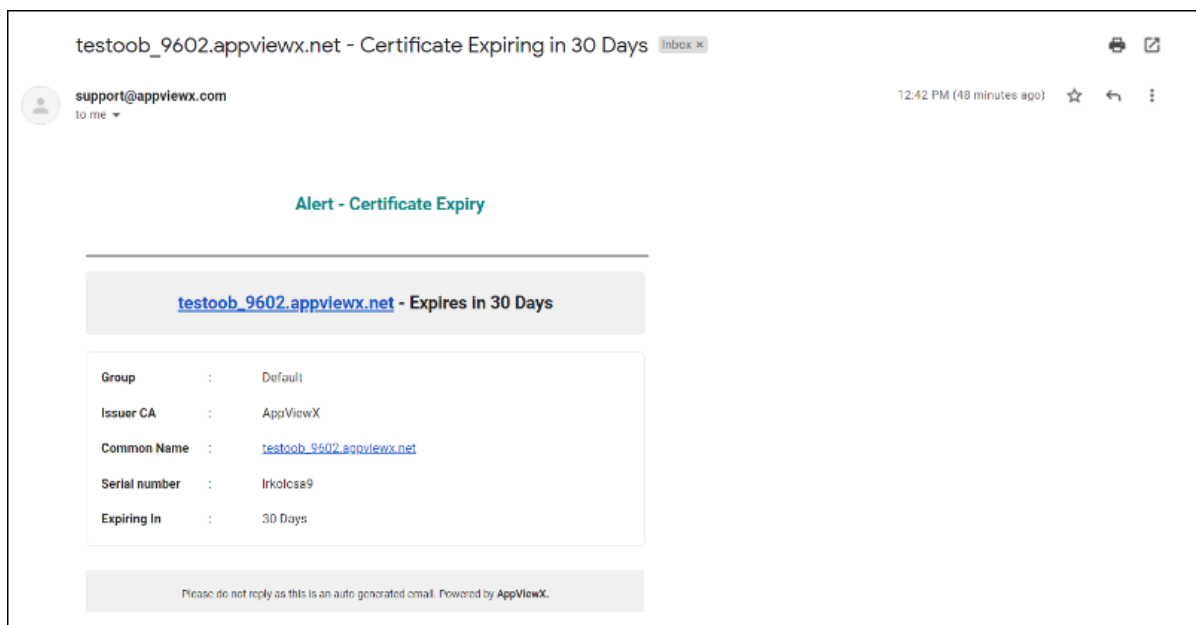
Field	Description
*Email Recipient	Select the required recipient of the notification. You can select: <ul style="list-style-type: none"> • Select all • Certificate Email - The notification will be sent to the email addresses associated with the certificate. • Certificate Group Email - The notification will be sent to the entire certificate group to which the certificate belongs.
*Report Format	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. <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 #add8e6; 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.

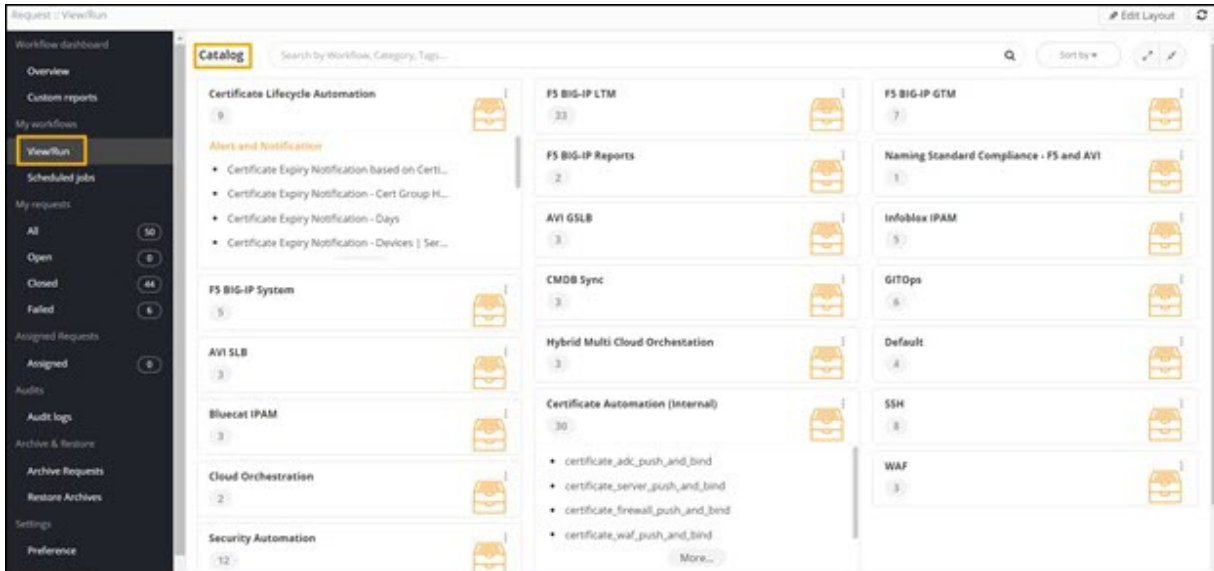




Certificate Expiry Notification - Devices | Servers

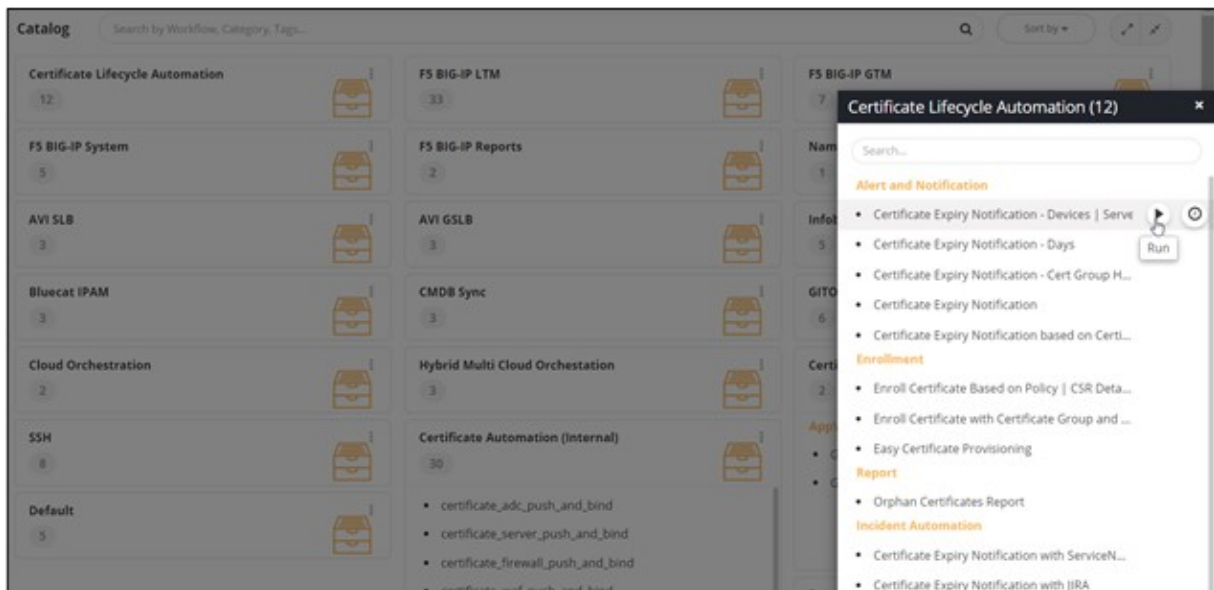
This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

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.

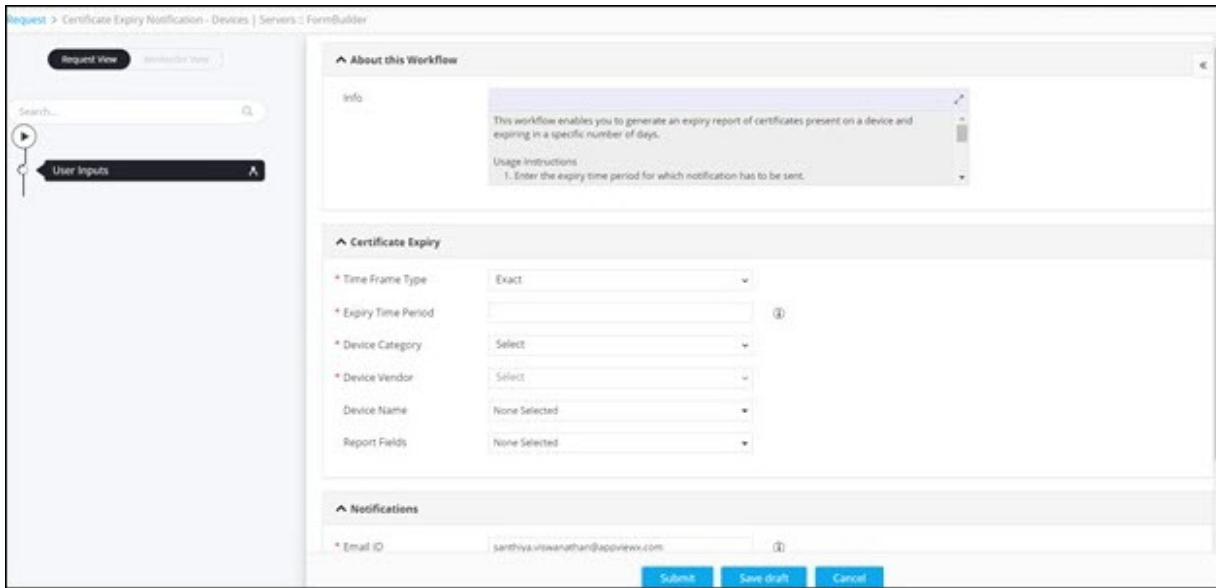


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

Certificate Expiry	
* Time Frame Type	Exact
* Expiry Time Period	
* Device Category	Select
* Device Vendor	Select
Device Name	None Selected
Report Fields	None Selected

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 #00a0e3; 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	<p>Select the device category for the report from the dropdown list.</p>
*Device Vendor	<p>Select the device vendor for the report from the dropdown list.</p>
Device Name	<p>Select the specific device for the report.</p>
Report Fields	<p>Select the report fields to be displayed in the report from the dropdown list.</p>
<p>All Asterisk (*) marked fields are mandatory.</p>	

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



^ Notifications

* Email ID ⓘ

CC Email ID ⓘ

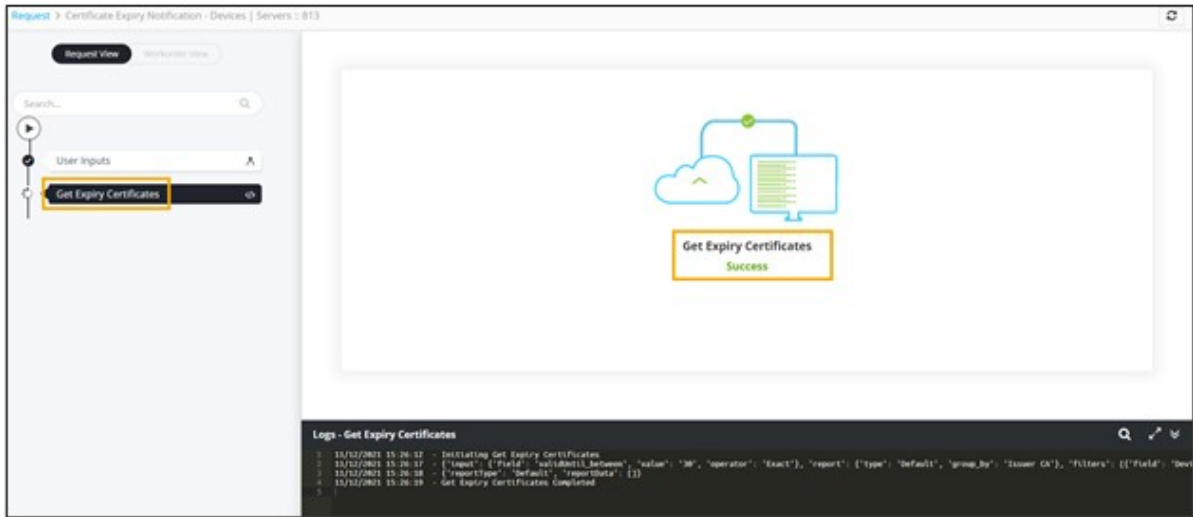
* Report Format Email Content CSV Attachment

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

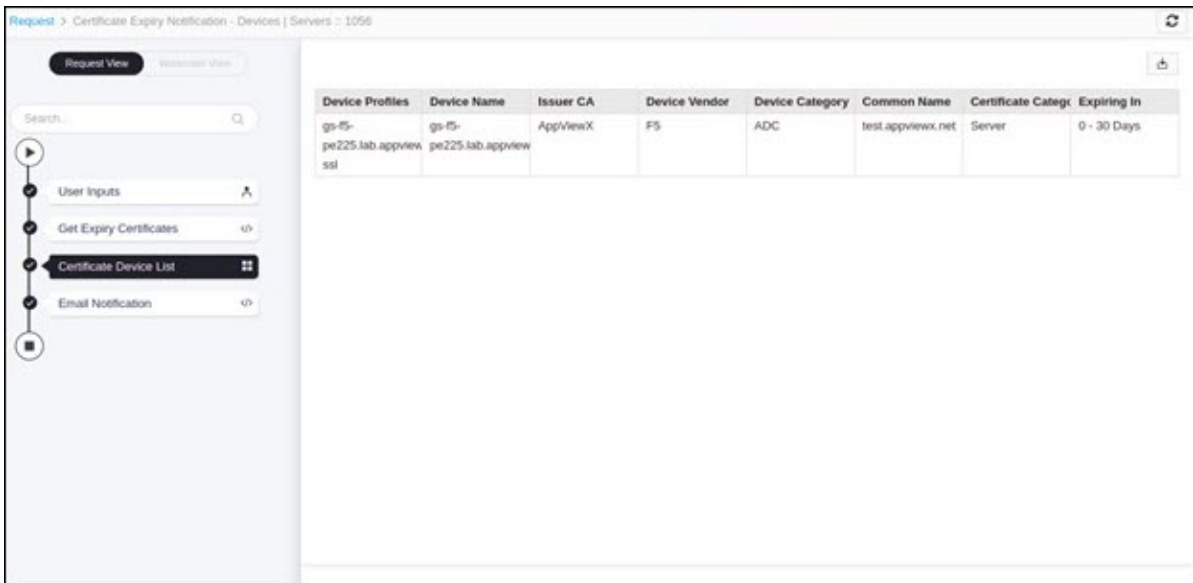
Field	Description
*Email ID	<p>Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses.</p> <div style="border: 1px solid #0070c0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: The email id of the logged in user is 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 #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**.

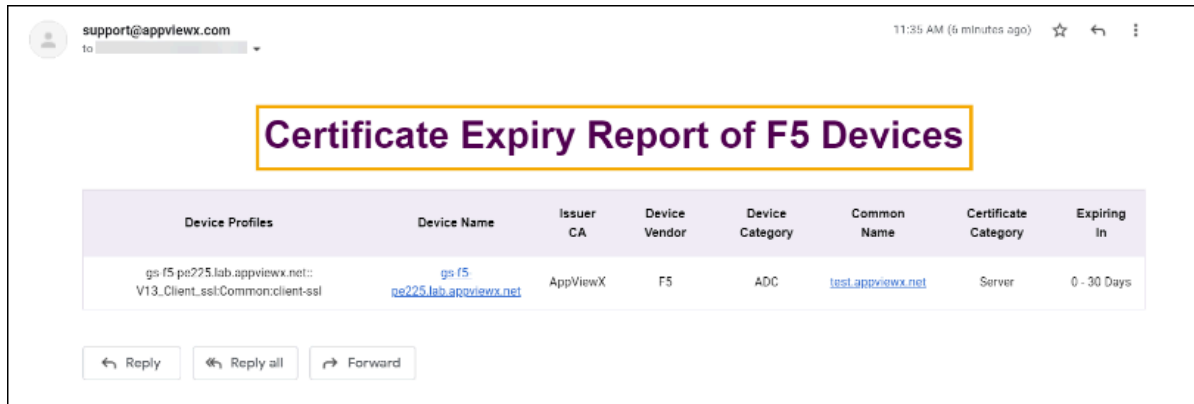
- Get Expiry Certificates task completed.



- Certificate Device list generated.



- Email report received.

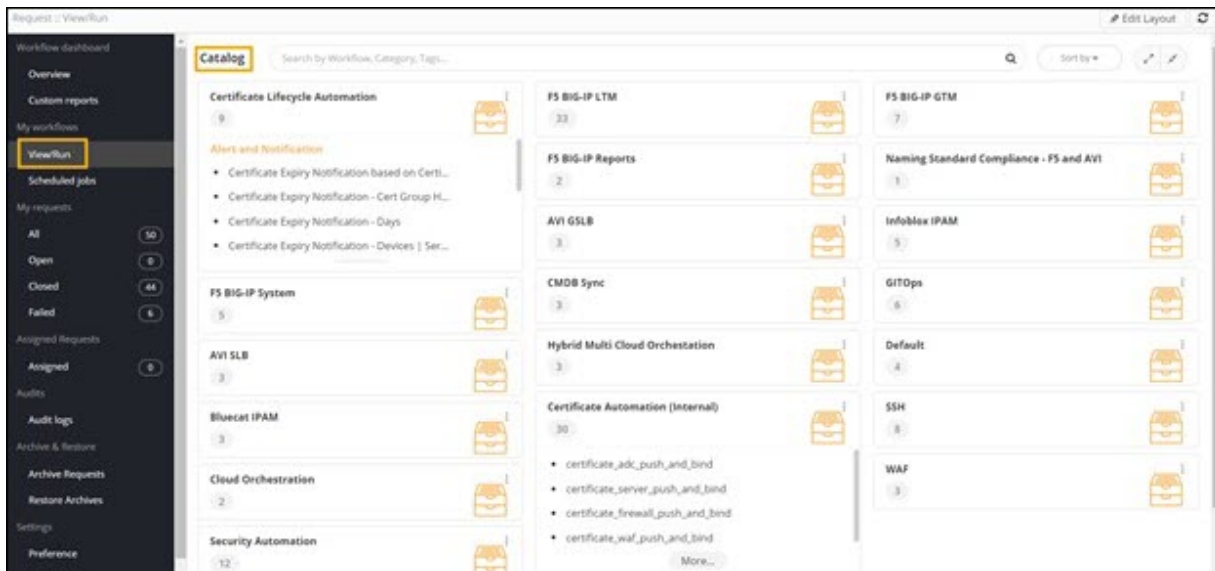


Certificate Expiry Notification


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.

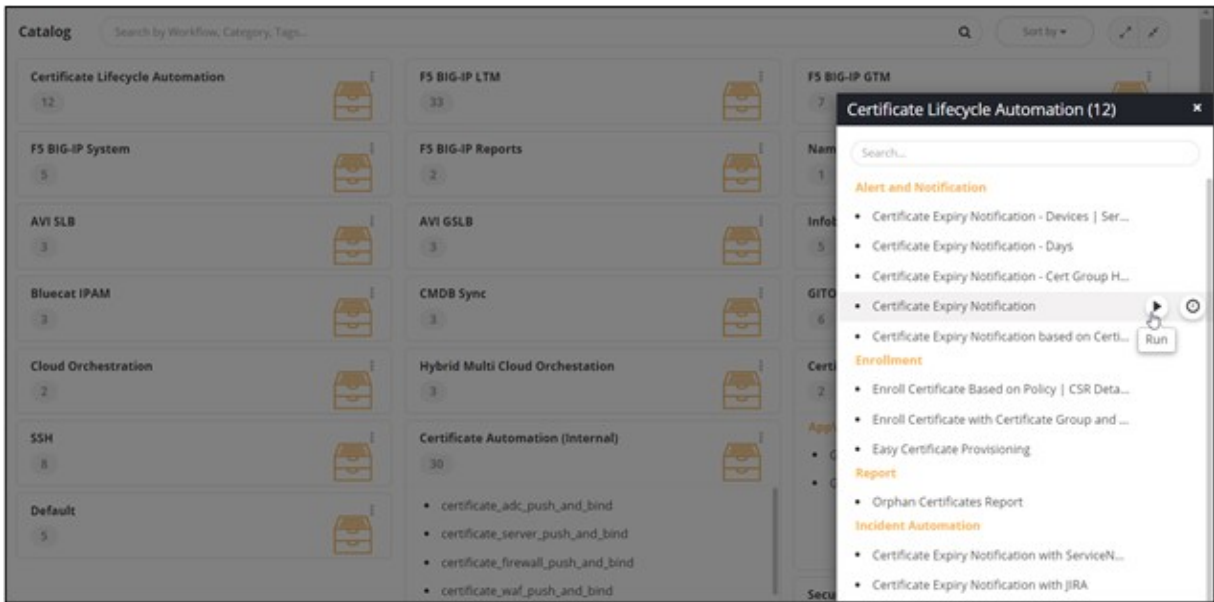
To trigger this workflow:


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



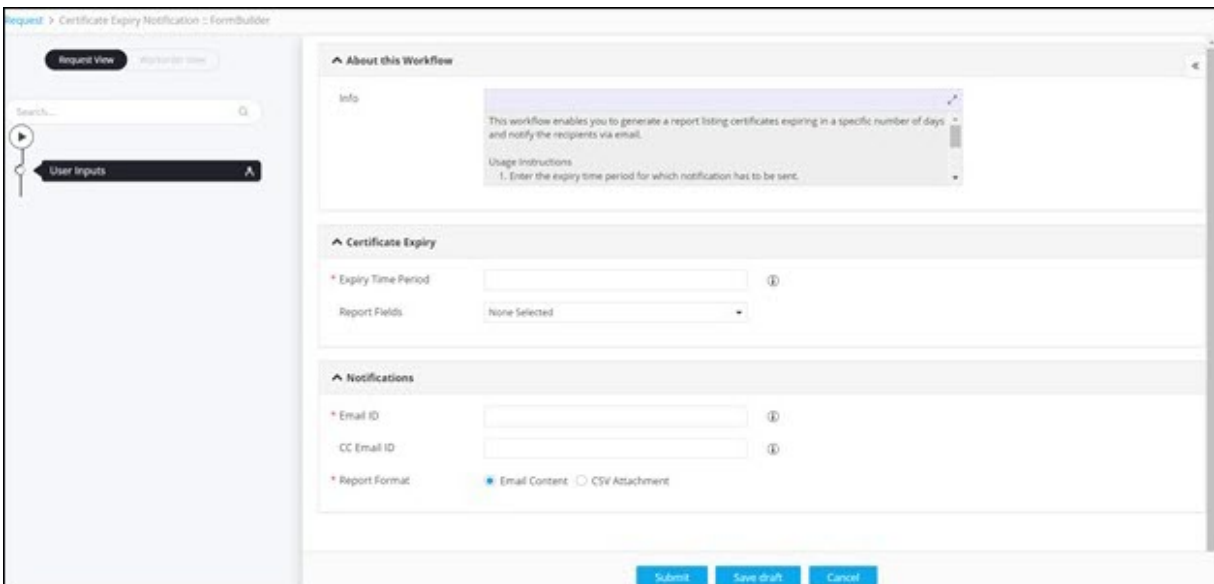
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.

- 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.




- 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	<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 #007bff; 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.



The screenshot displays the 'Request View' for a 'Certificate Expiry Notification - SP' workflow. The workflow steps are: User Inputs, Get Expiry Certificates (highlighted), and Email Notification. The main canvas shows a diagram of the 'Get Expiry Certificates' task with a 'Success' status. Below the canvas, the logs for the 'Get Expiry Certificates' task are visible, showing the following entries:

```

Logs - Get Expiry Certificates
1 11/12/2021 14:16:33 - Initializing Get Expiry Certificates
2 11/12/2021 14:16:48 - [Event Type: 'Default', 'EventData': [{"Serial number": "xxxxxxxx", "Error OK": "Approved", "Common Name": "testlab_0396_appview.net", "Group": "Default"}]]
3 11/12/2021 14:16:48 - Get Expiry Certificates Completed

```

- Email notification received with report as email content.

Certificate Expiry Report in 30 Days Inbox X

support@appviewx.com
to [redacted]

2:16 PM (0 minutes ago) ☆ ↶ ⋮

Certificate Expiry Report

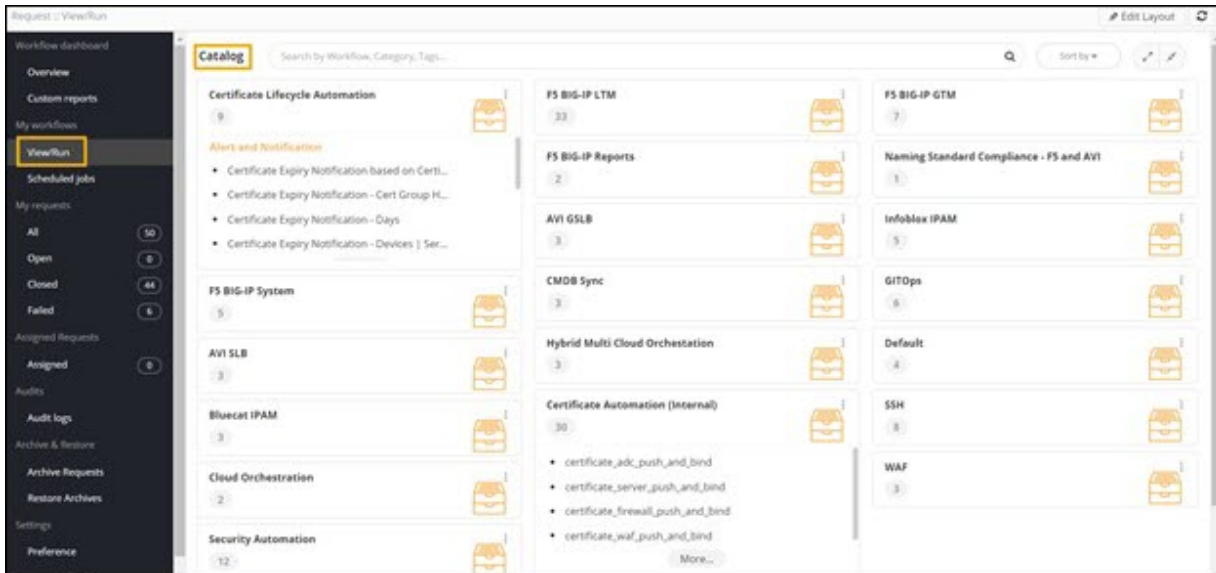
Serial number	Issuer CA	Common Name	Group	Expiring In
csisen56u	AppViewX	testoob_6196.appviewx.net	Default	30 Days
jrtpjxrva	AppViewX	testoob_1907.appviewx.net	Default	30 Days
rbckrvo1o	AppViewX	testoob_5381.appviewx.net	Default	30 Days
3pc9ahubn	AppViewX	testoob_2055.appviewx.net	Default	30 Days
v88rxpcnb	AppViewX	testoob_7197.appviewx.net	Default	30 Days
ljdwv8ace	AppViewX	testoob_5830.appviewx.net	Default	30 Days
69swwssec	AppViewX	testoob_8342.appviewx.net	Default	30 Days
txyknmfe1	AppViewX	testoob_9973.appviewx.net	Default	30 Days
9wpmjt9nd	AppViewX	testoob_6657.appviewx.net	Default	30 Days
6cst2u3nn	AppViewX	testoob_9586.appviewx.net	Default	30 Days



Update Certificate Attributes

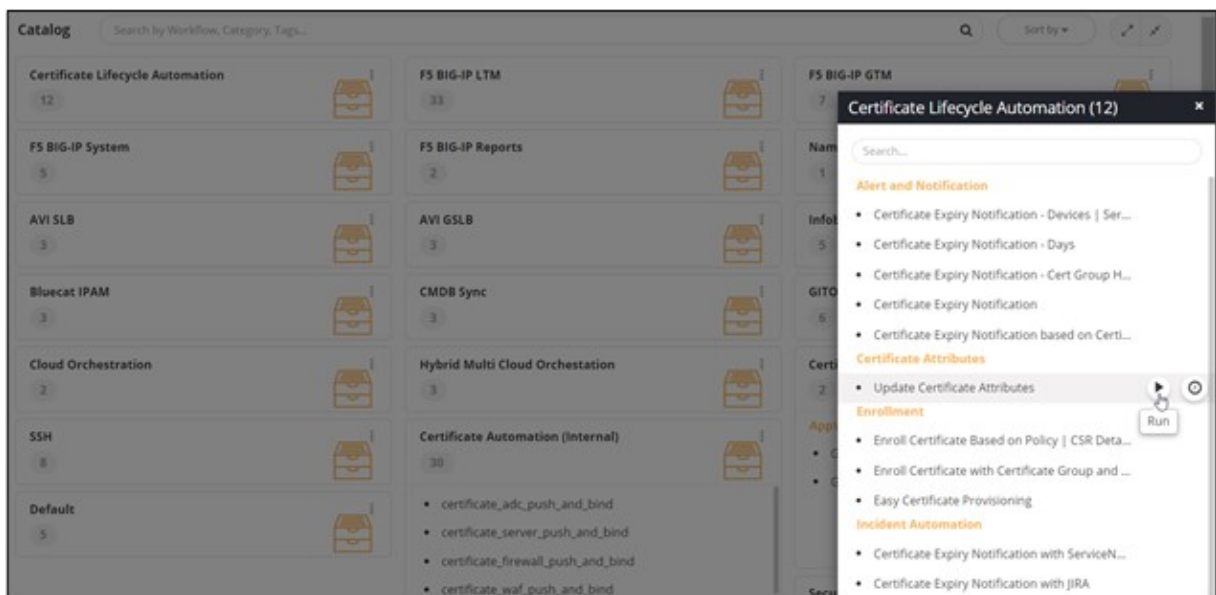
This workflow allows you to update the certificate attributes in bulk.

To trigger this workflow:

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







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



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

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

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

Field	Description
* Certificate Filter Choice	<p>Select the required checkbox to fetch</p> <ul style="list-style-type: none"> • All certificates <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-bottom: 10px;">  Note: This is the default selection. </div> <ul style="list-style-type: none"> • Based on Criteria <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px;">  Note: Selecting this option will fetch certificates based on criteria such as certificate group and certificate category. </div>
* Certificate Group	<p>Select the appropriate certificate group from the dropdown list.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when you select the Based on Criteria option in Certificate Filter Choice. </div>
* Certificate Category	<p>Select the appropriate certificate category from the dropdown list.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;">  Note: This field is displayed only when you select the Based on Criteria option in Certificate Filter Choice. </div>

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

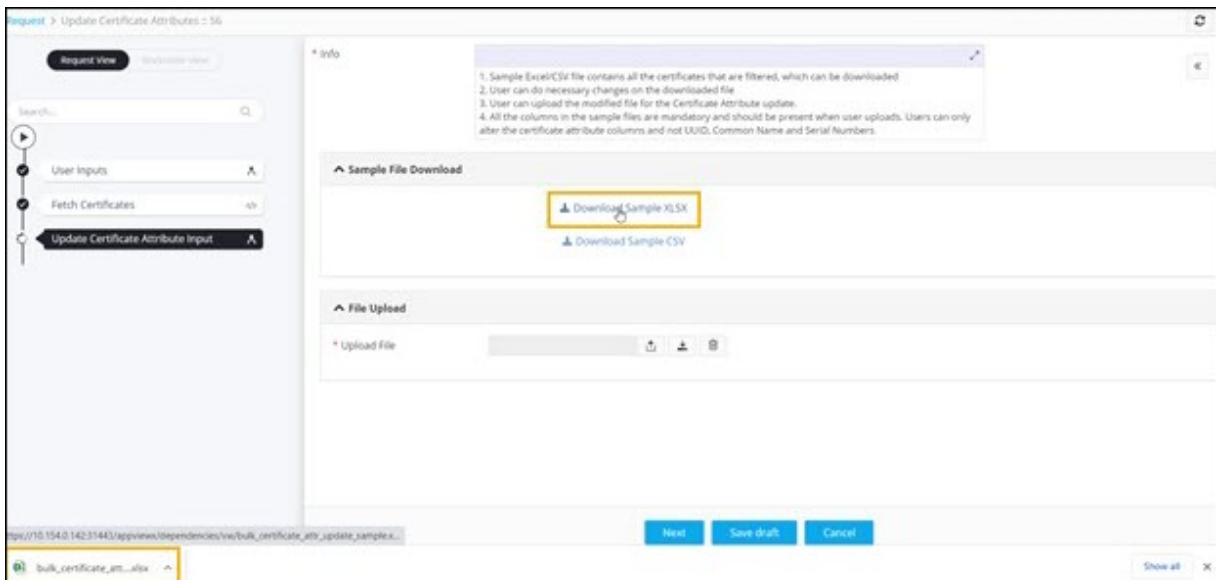
5. Click **Submit**.


Fetch Certificates task is executed.

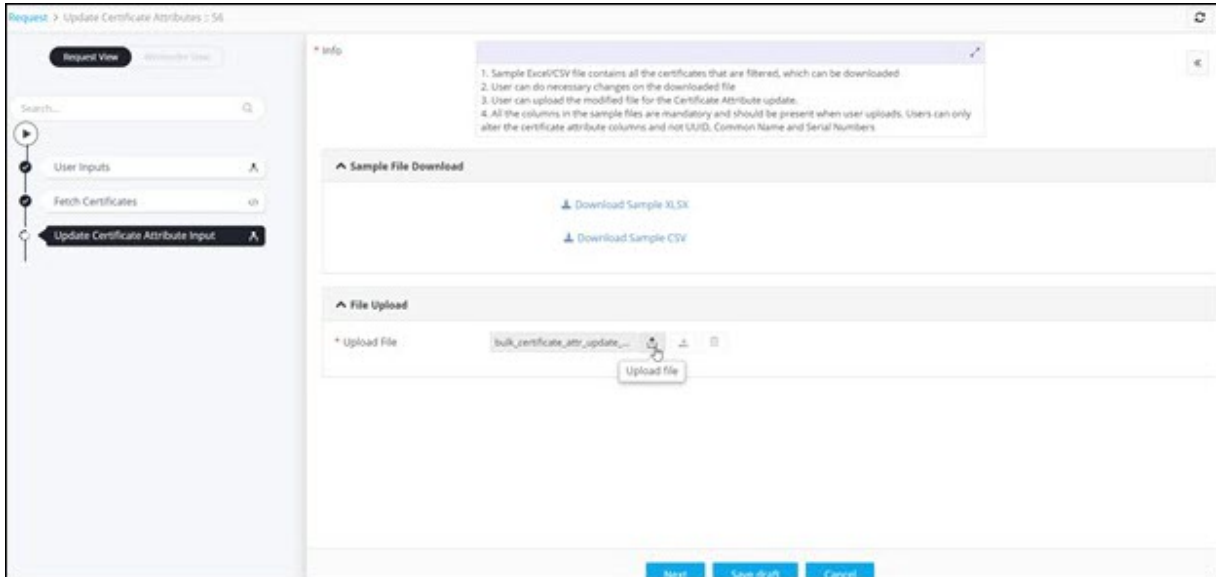


6. Select the appropriate option for downloading the file as a CSV or Excel file.

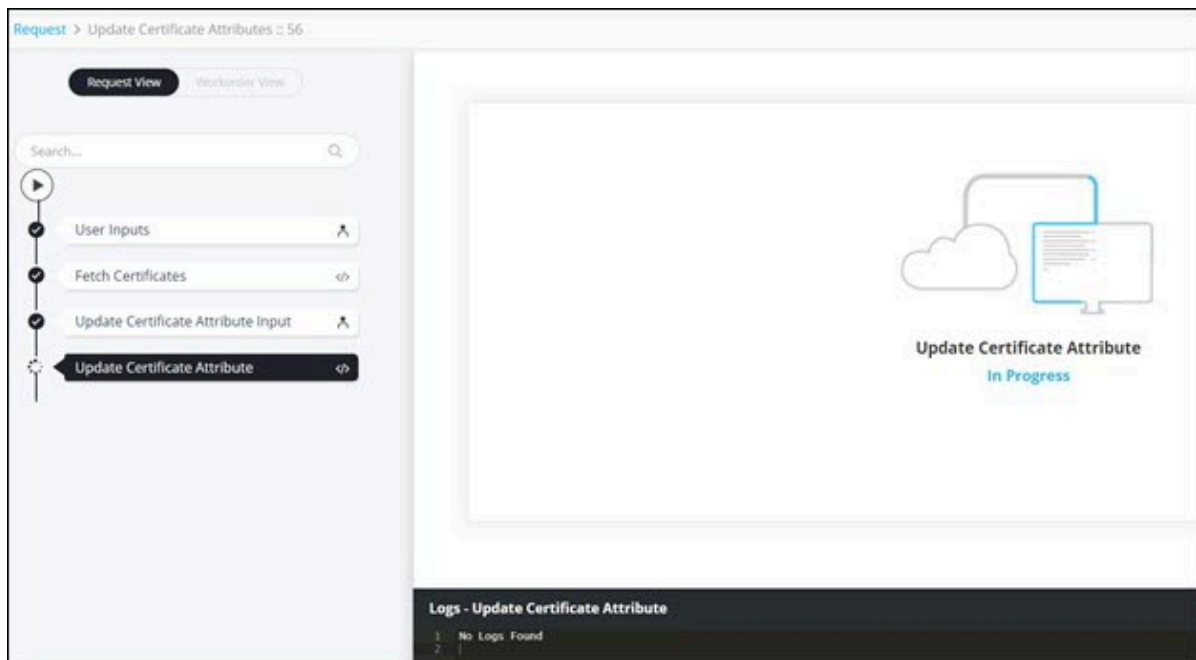
The file is downloaded to your device.




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  .

Request > Update Certificate Attributes : 59

Request View

Search...

User Inputs

Fetch Certificates

Update Certificate Attribute Input

Update Certificate Attribute

Update Certificate Status

Status	Details	Common Name	Serial Number
Success	updated certificate with cert attributes successfully	cert001.appviewx.com	96:7A:70:D5:56:C3:A9:98:B7:67:9F:37:18:97:
Success	updated certificate with cert attributes successfully	cert002.appviewx.plus	
Success	updated certificate with cert attributes successfully	cert003.appviewx.appviewx.com	7AFA:CD:57:E7:1B:30:10:8D:8C:D7:99:FD:CE
Success	updated certificate with cert attributes successfully	coobtest.appviewx.plus	05:22:44:EB:89:47:31:4E:2C:3A:9D:98:71:9E:
Success	updated certificate with cert attributes successfully	test.appviewx.com	7A:F2:94:2A:11:52:16:DD:ED:2C:6A:AE:9E:D6
Success	updated certificate with cert attributes successfully	test00b	F9:C8:28:50:FC:50:A9:28:DD:8C:75:11:3A:4B
Success	updated certificate with cert attributes successfully	test00b_1.appviewx.net	q0f0ck23u
Success	updated certificate with cert attributes successfully	test00b_2.appviewx.net	5jxfjako
Success	updated certificate with cert attributes successfully	test00b_3.appviewx.net	ipny9eu6k
Success	updated certificate with cert attributes successfully	test00b_4.appviewx.net	8ekzbww49
Success	updated certificate with cert attributes successfully	test00b_5.appviewx.net	bolbmuaqpy
Success	updated certificate with cert attributes successfully	test00b_6.appviewx.net	uwwrtfaw

- Email notification sent successfully.

Request > Update Certificate Attributes : 59

Request View

Search...

User Inputs

Fetch Certificates

Update Certificate Attribute Input

Update Certificate Attribute

Update Certificate Status

Email Notification



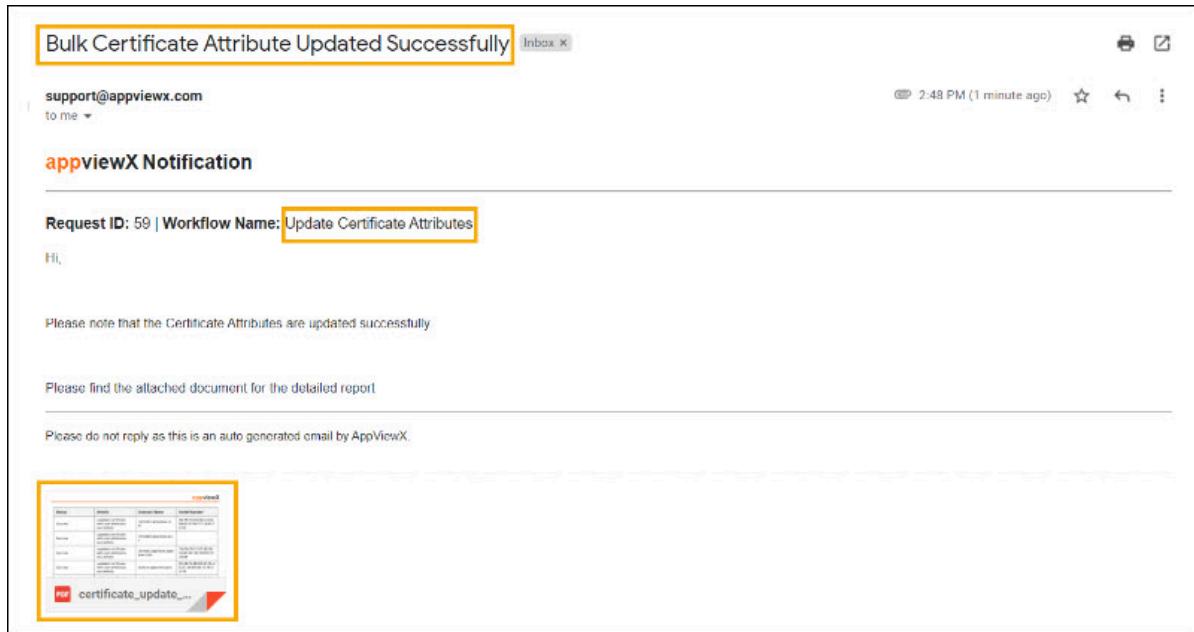
Email Notification
Success

Logs - Email Notification

```

11/12/2021 14:47:18 - Initiating Email Notification
11/12/2021 14:47:18 - Email to Uppared: Email Notification
11/12/2021 14:47:20 - Total recipients: 1
11/12/2021 14:47:20 - emailStatus:Success
Certificate update status: all
11/12/2021 14:47:20 - Send Email Successful: Email Notification
11/12/2021 14:47:20 - Email Notification Completed
    
```

- Email with report received.

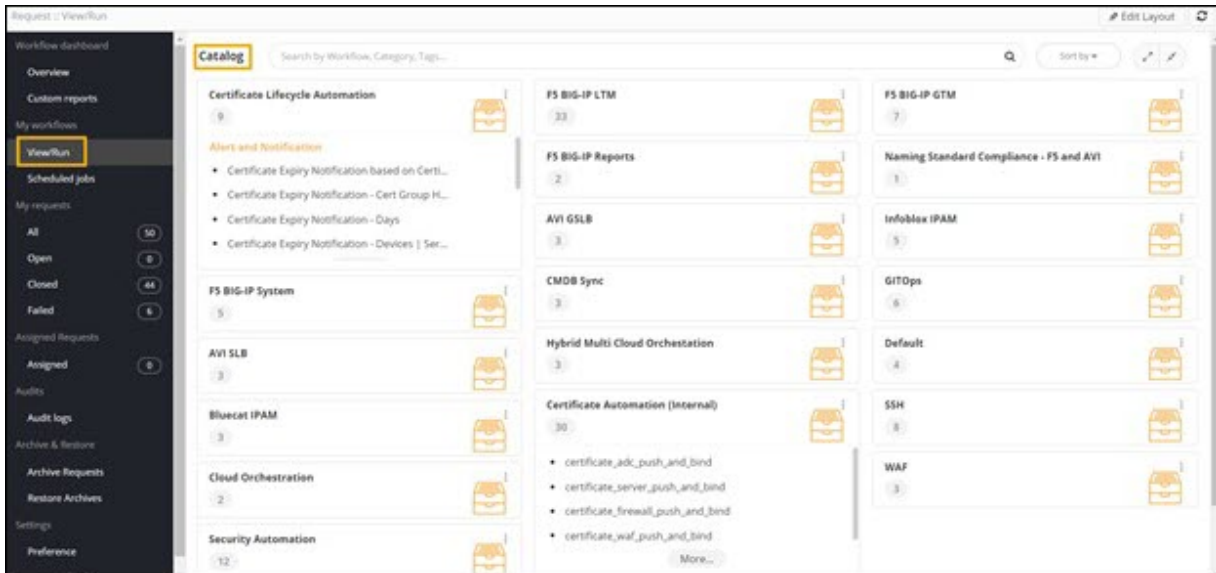




Certificate Expiry Notification with JIRA

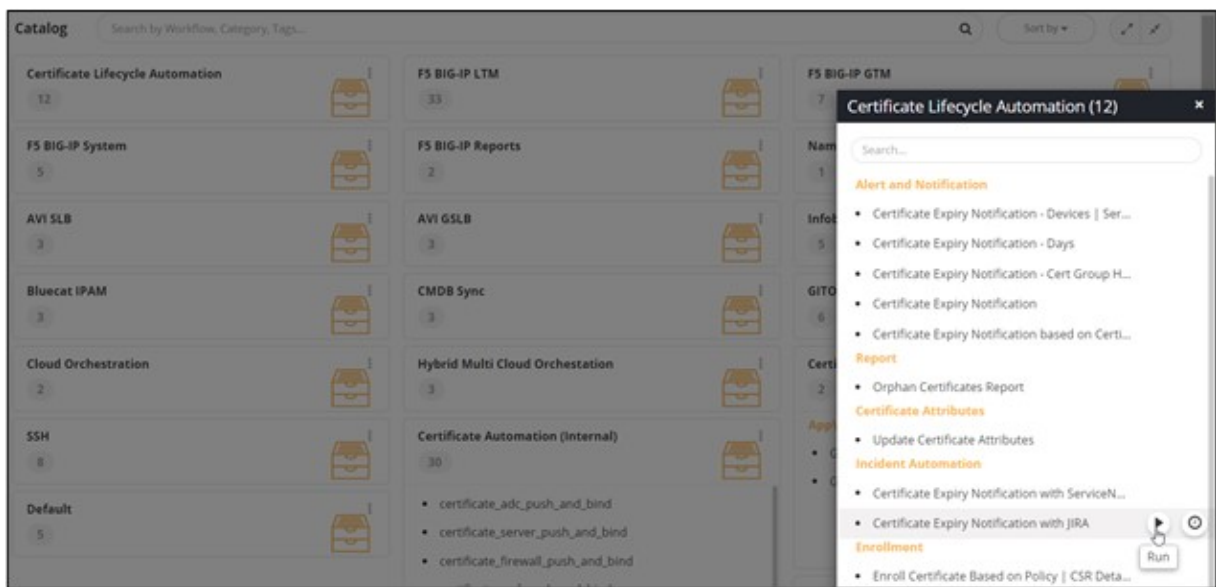
This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.


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.

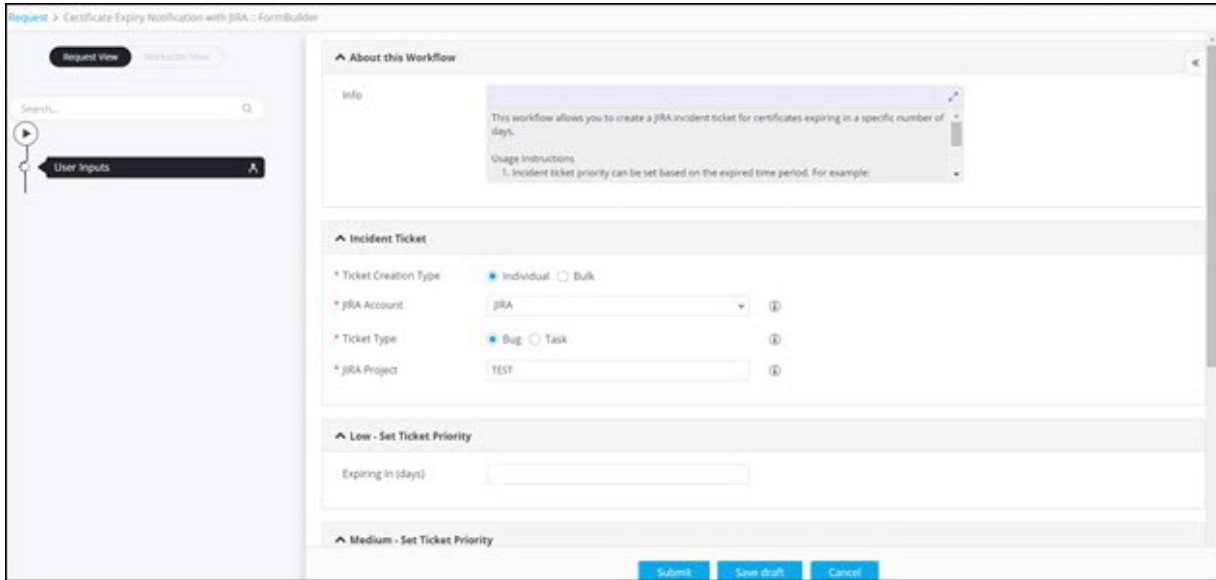


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

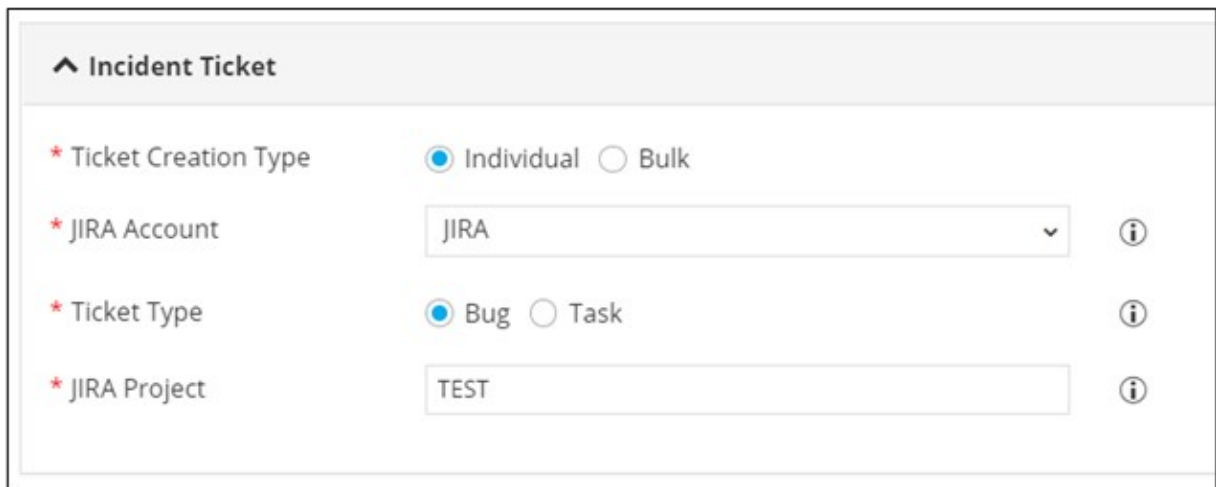


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.

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
<p>*Ticket Creation Type</p>	<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;"> <p> Note: Individual is the default selection.</p> </div>

Field	Description
* 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.	

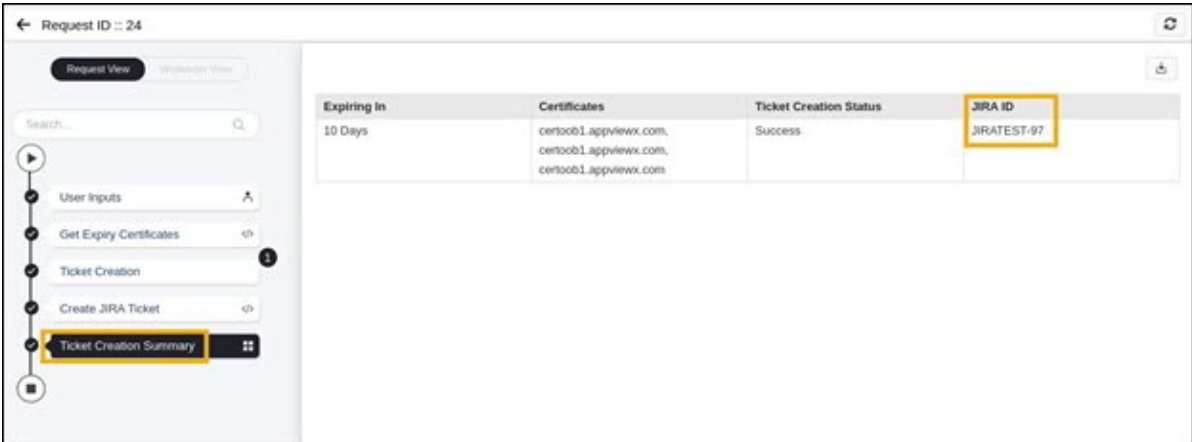
- Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
- Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for 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.



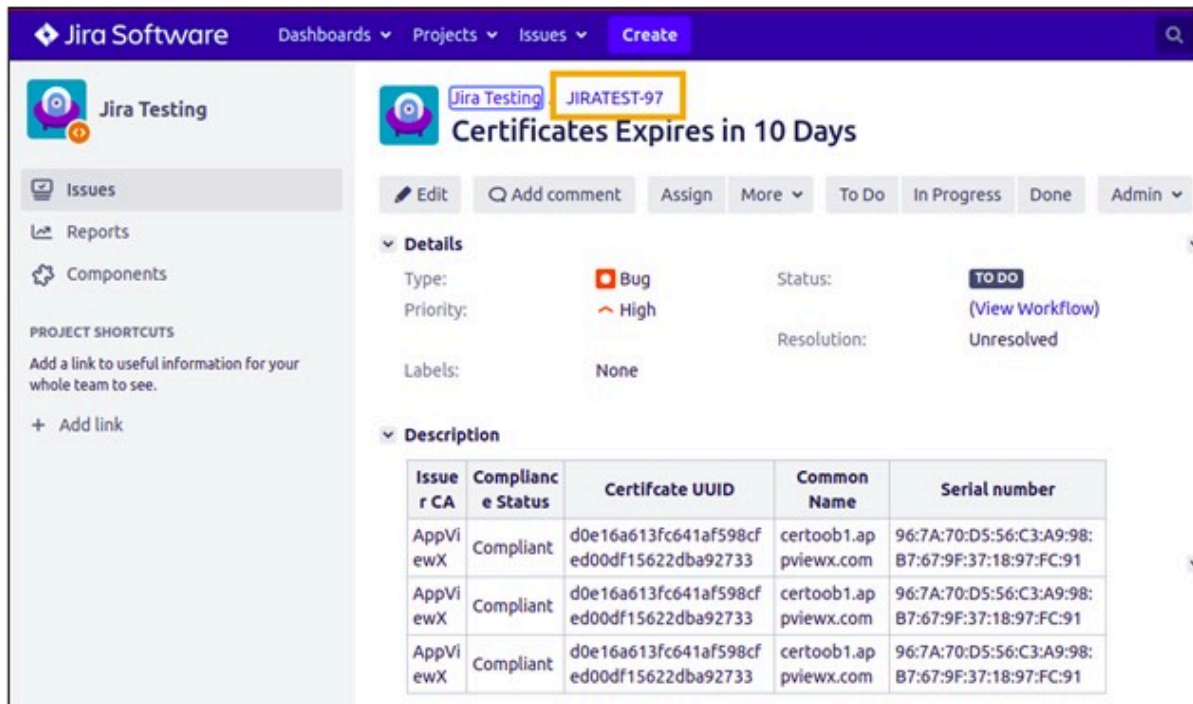
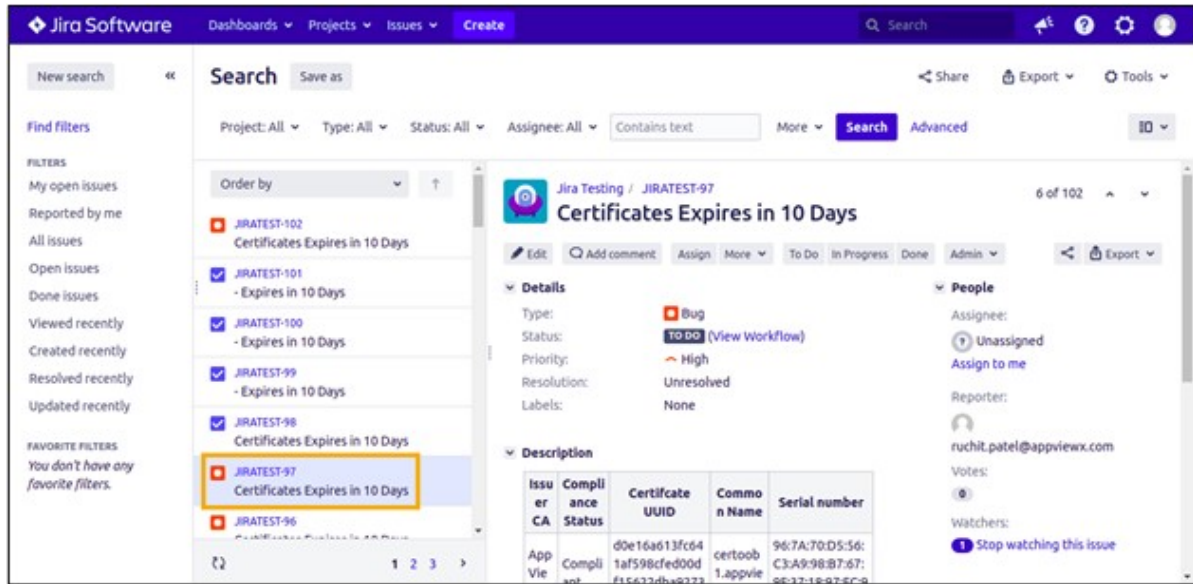
Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

- Click **Submit**.

- JIRA ticket creation Summary.



- Ticket created on Jira.

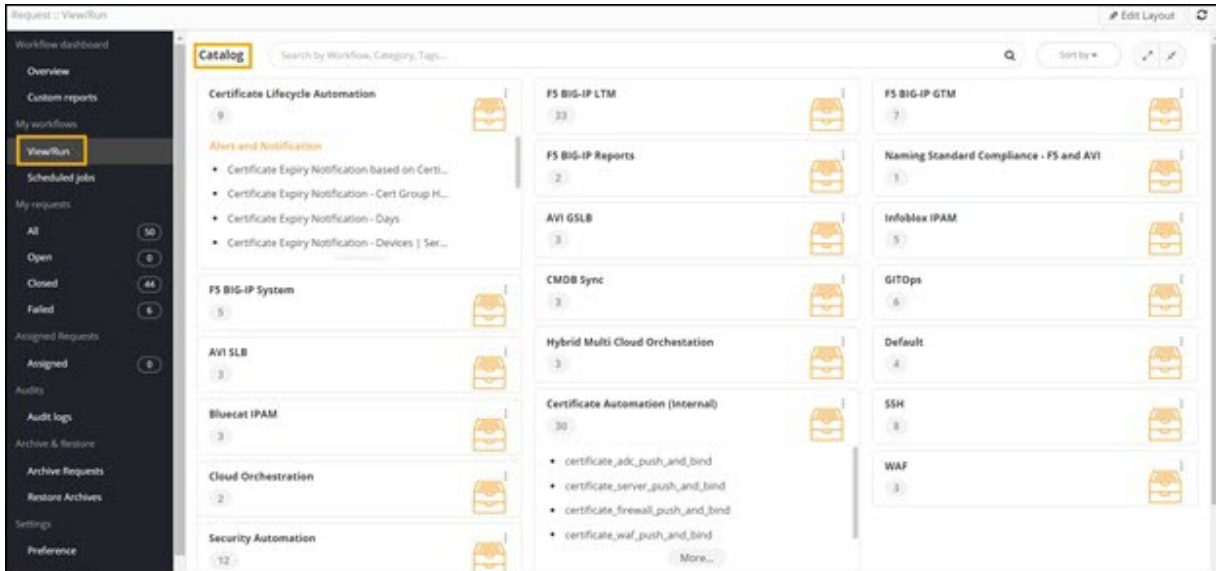




Certificate Expiry Notification with ServiceNow

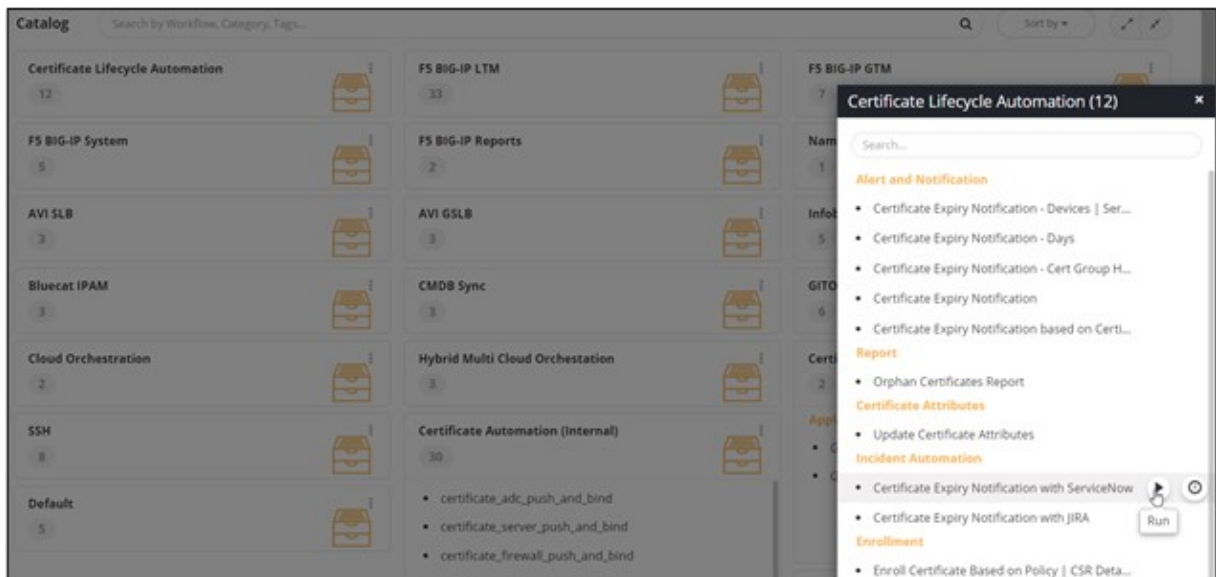
This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.


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.

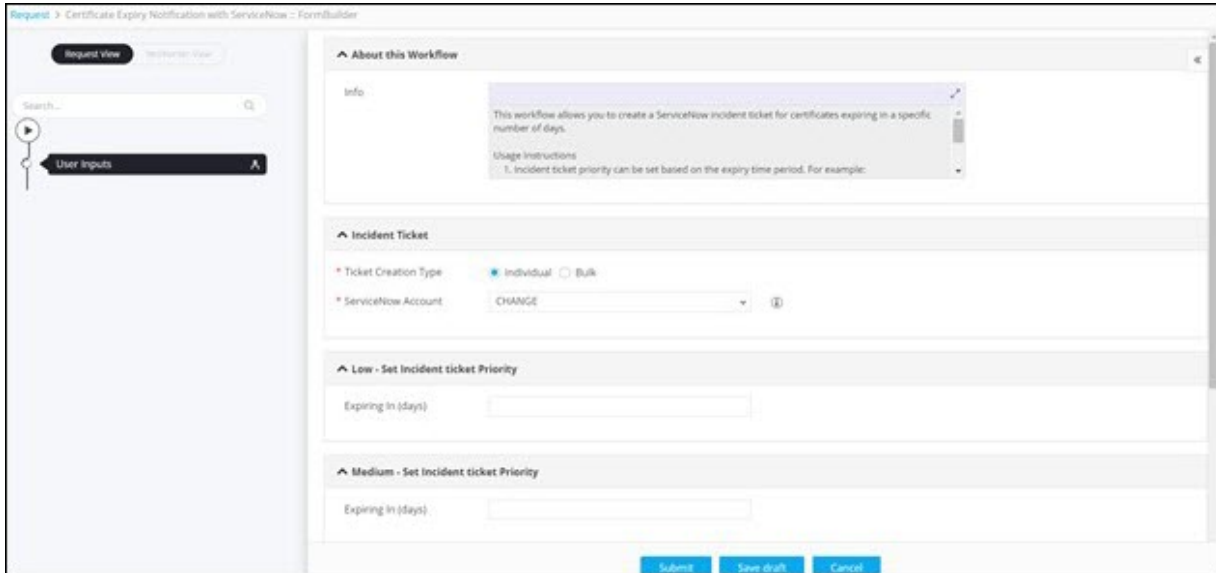


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

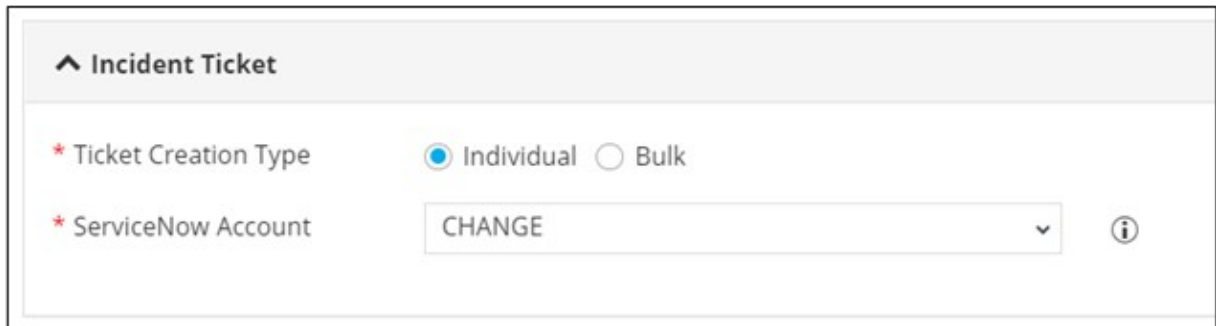


 **Tip:** You can also search for the workflow by typing the workflow name in the search bar.


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;"> <p> Note: Individual is the default selection.</p> </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.	

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

 **Note:** This is a mandatory field.

10. Click **Submit**.

- Incident Creation Summary



- Incident ticket created on ServiceNow.

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

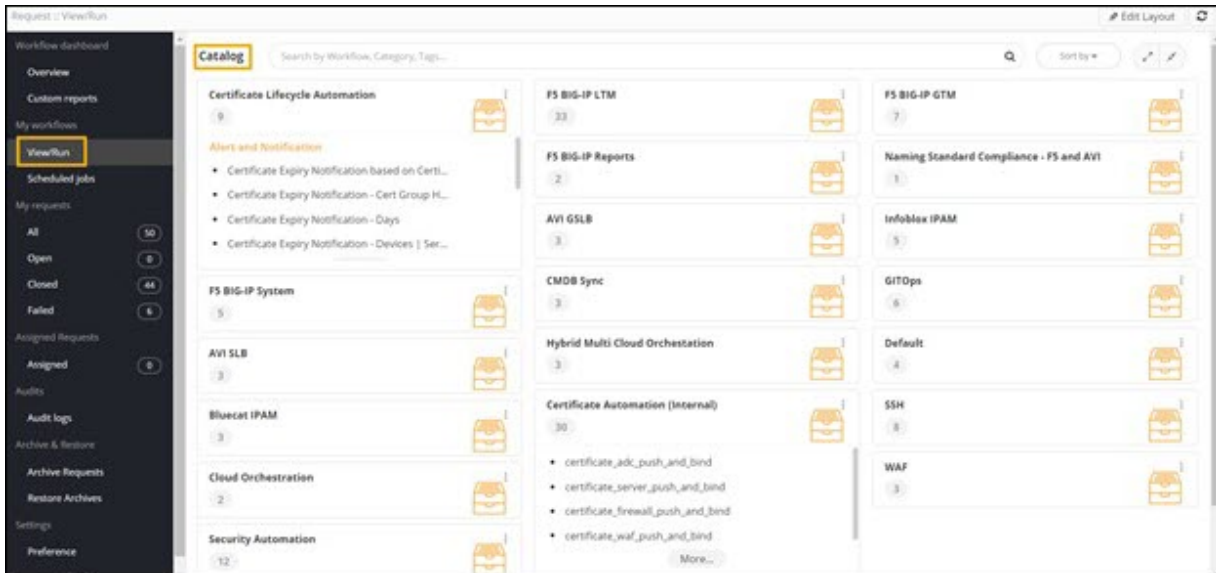
	Number	Caller	Short description	Category	Priority	State	Assignment group	Assigned to	
	INC0014751	(empty)	certtoob1.appviewx.com - Expires in 10 Days	Inquiry / Help	1 - Critical	New	(empty)	(empty)	2021 03:51
	INC0014750	(empty)	Certificates - Expires in 10 Days	Inquiry / Help	1 - Critical	New	(empty)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



Orphan Certificates Report

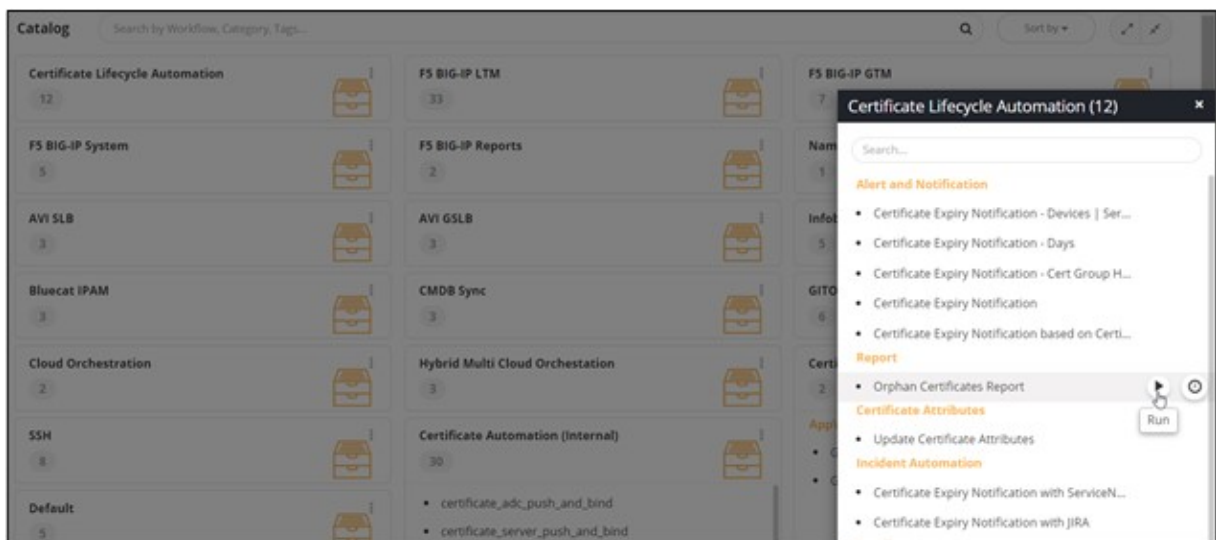
This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.


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.

The screenshot shows the 'Orphan Certificates Report' FormBuilder interface. It features a sidebar with 'Request View' and 'Workflow View' tabs, a search bar, and a 'User Inputs' section. The main content area is divided into three sections: 'About this Workflow' (with an info box and usage instructions), 'Device Information' (with dropdowns for Category, Vendor, Name, and Device Certificate Fields), and 'Notifications' (with fields for Email ID, CC Email ID, and Report Format). At the bottom, there are 'Submit', 'Save draft', and 'Cancel' buttons.

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

This close-up view of the 'Device Information' section shows four dropdown menus. The 'Category' and 'Vendor' fields are both set to 'Select'. The 'Name' and 'Device Certificate Fields' fields are both set to 'None Selected'.

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.



^ 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	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses.  Note: The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field. Comma separated values can be entered for multiple email addresses.
* Report Format	Select the required checkbox to send the report as: <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 Orphan Certificates task executed.

The screenshot shows a workflow execution interface for 'Orphan Certificates Report : 67'. The workflow steps are: User Inputs, Get Orphan Certificates (highlighted), Orphan Certificates List, and Email Notification. The main area displays a 'Get Orphan Certificates Success' message with a cloud and server icon. Below the main area, a log entry shows the task completion details.

```

Logs - Get Orphan Certificates
1 11/16/2021 11:48:32 Initiating Get Orphan Certificates
2 11/16/2021 11:48:33 Filters: { 'device_category': 'ADC', 'device_vendor': 'FS', 'filters': [{ 'field': 'device_profiles', 'operator': 'is', 'value': '' }, { 'field': 'common_name', 'operator': 'is', 'value': '' } ] }
3 11/16/2021 11:48:34 Get Orphan Certificates completed
    
```

- Orphan Certificates List generated.

The screenshot shows the workflow execution interface for 'Orphan Certificates Report : 812'. The workflow steps are: User Inputs, Get Orphan Certificates, Orphan Certificates List (highlighted), and Email Notification. The main area displays a table of orphan certificates.

Issuer CA	Device Name	Device Profiles	Device Category	Device Vendor	Serial number	Common Name
OTHERS	gs-fs-pe225.lab.appviewx.net		ADC	FS	89-BE-6F-8A-89-77-48-69	F5v12_gu8M5A20485H
AppViewX	Citrix85		ADC	Citrix	3A-F9-F0-C4-22-12-C2-AD	testeasy25.appviewx.co
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	3A-F9-F0-C4-22-12-C2-AD	testeasy25.appviewx.co
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	F2-5E-C7-0D-84-76-2F-68	Apr120AW9Linux.com
AppViewX	Apache30	Server	Server	Apache	F2-5E-C7-0D-84-76-2F-68	Apr120AW9Linux.com
OTHERS	gs-fs-pe225.lab.appviewx.net		ADC	FS	DA-F4-85-FF-D1-53-38-A4	admserver.com
OTHERS	gs-fs-pe225.lab.appviewx.net		ADC	FS	15-73-51-D9	testabd.lab.appviewx.net
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	6D-9C-F9-7E-5B-10-F3-8A	vmflaskapp.appviewx.net
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	E7-D6-65-1B-FF-02-1E-19	testeasyjav5.appviewx.net
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	0D-5B-64-A1-7B-ED-C6-87	1024
AppViewX	gs-fs-pe225.lab.appviewx.net		ADC	FS	F9-4E-C0-64-36-49-3B-08	testeasyavwrth51.appviewx.net
OTHERS	gs-fs-pe225.lab.appviewx.net		ADC	FS	49-B1-F3-69-5D-B0-64-93	ApacheCustomDir.appviewx.net

- Email notification received with report as email content.

Orphan Certificate Report of F5 Devices Inbox x

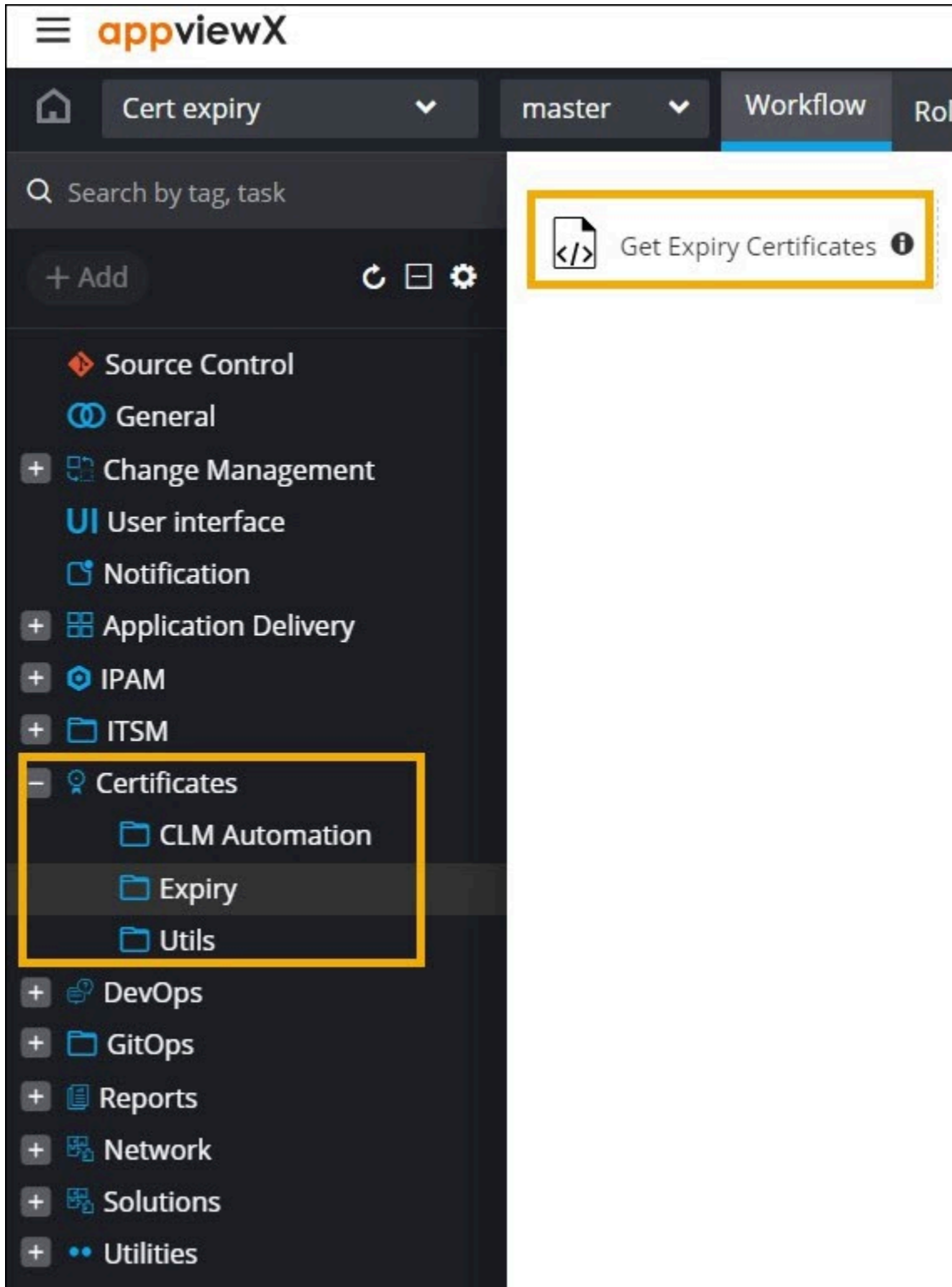
support@appviewx.com 3:21 PM (1 minute ago) ☆ ↶ ⋮

Orphan Certificate Report of F5 Devices


Issuer CA	Device Name	Device Profiles	Device Category	Device Vendor	Serial number	Common Name
OTHERS	qs-f5-pe225.lab.appviewx.net	-	ADC	F5	89:BE:6F:BA:89:77:48:69:B7:9F:50:5D:2B:C9:11:28	F5v12_qushRSA2048SHA160.appviewx.com
AppViewX	Citrix85	-	ADC	Citrix	3A:F9:F0:C4:22:12:C2:AD:45:15:D3:47:66:4E:0C:AD	testeasy25.appviewx.com
AppViewX	qs-f5-pe225.lab.appviewx.net	-	ADC	F5	3A:F9:F0:C4:22:12:C2:AD:45:15:D3:47:66:4E:0C:AD	testeasy25.appviewx.com
AppViewX	qs-f5-pe225.lab.appviewx.net	-	ADC	F5	F2:5E:C7:0D:84:76:2F:68:5F:53:FA:D2:04:C4:8E:78	April20AW SLinux.com
AppViewX	Apache80	-	Server	Apache	F2:5E:C7:0D:84:76:2F:68:5F:53:FA:D2:04:C4:8E:78	April20AWSLinux.com
OTHERS	qs-f5-pe225.lab.appviewx.net	-	ADC	F5	DA:F4:85:FF:D1:93:38:A4	admserver.com

Chapter 5: Certificate Expiry Notification task

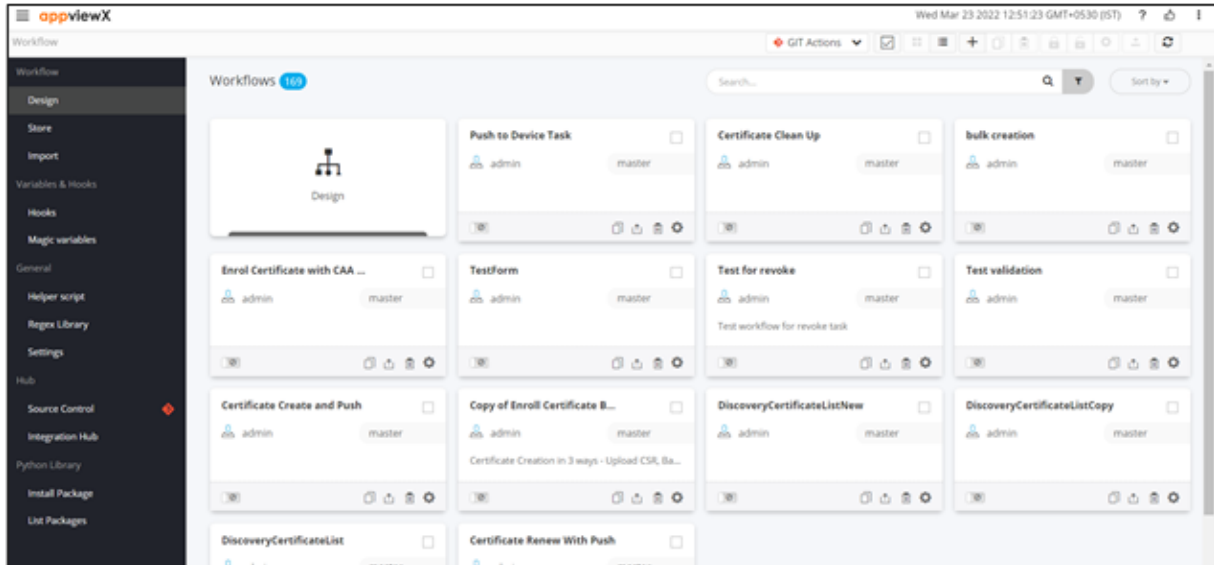
You can design a custom workflow for receiving certificate expiry notifications using the prebuilt task for getting expiry certificates available in the Workflow Studio. The OOB script task for getting expiry certificates can be found under **Certificates**, in the **Expiry** folder in the Workflow Studio.



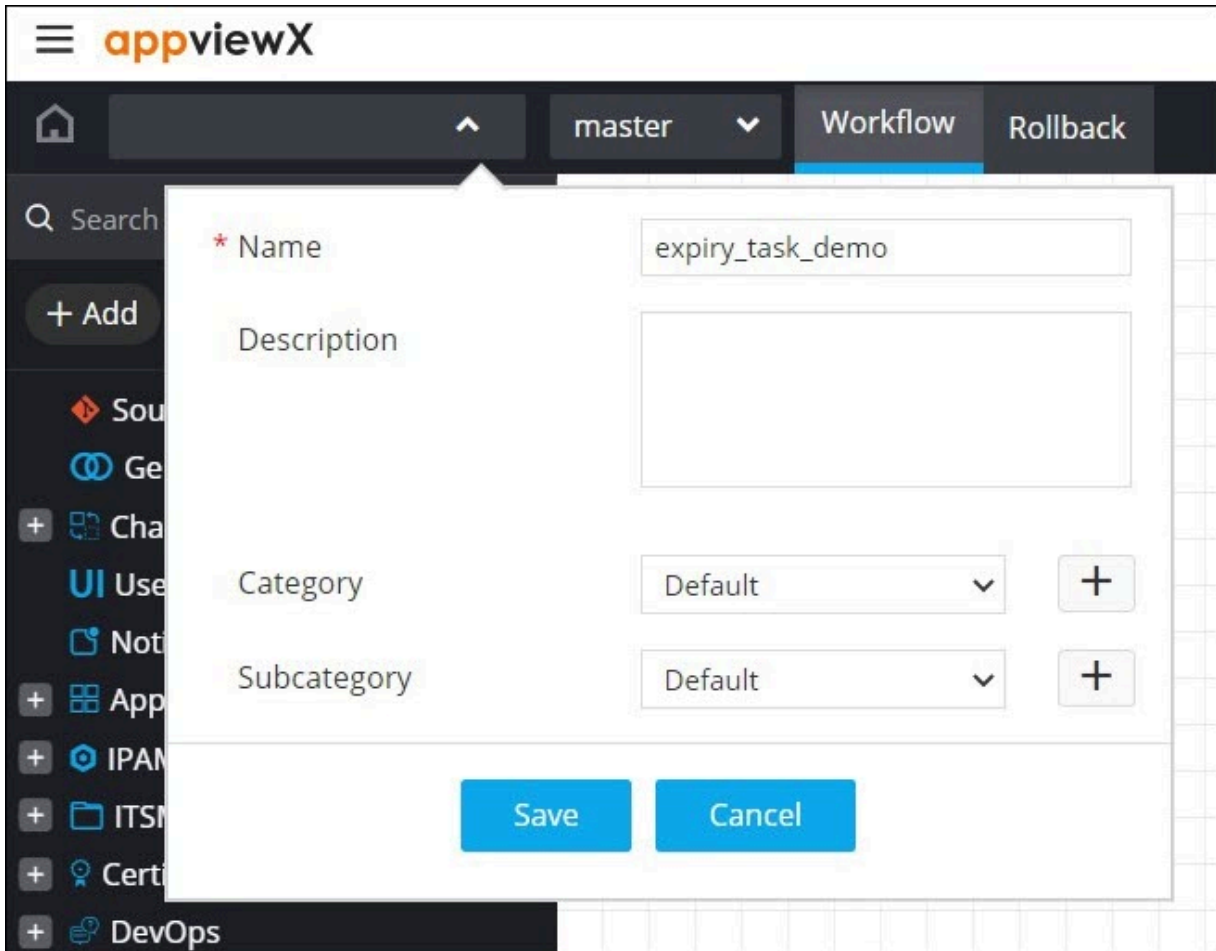
To design a custom workflow using the **Get expiry certificates** task

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

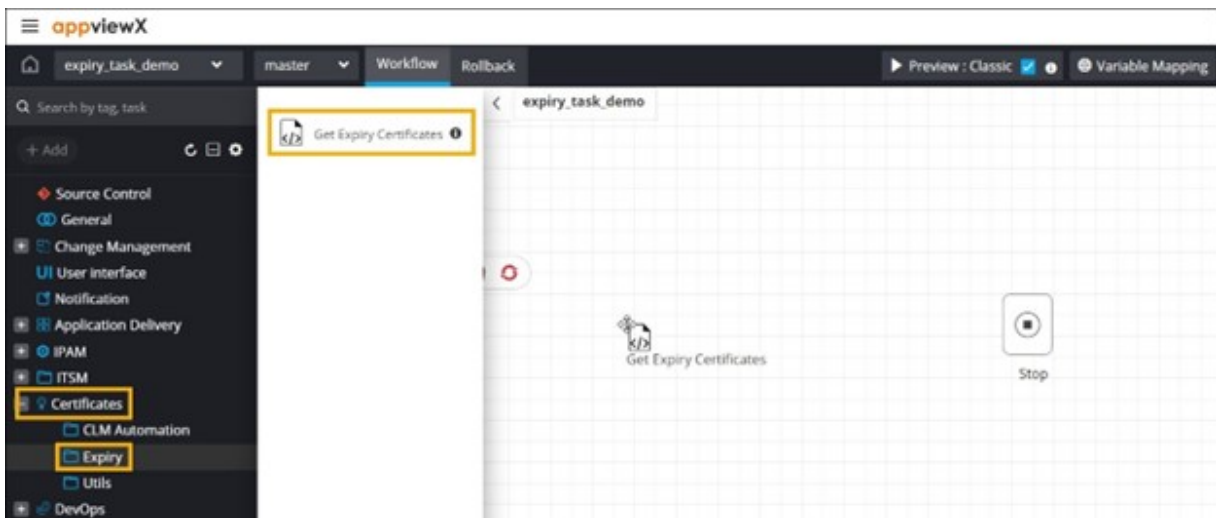
The **Workflow** inventory page is displayed.



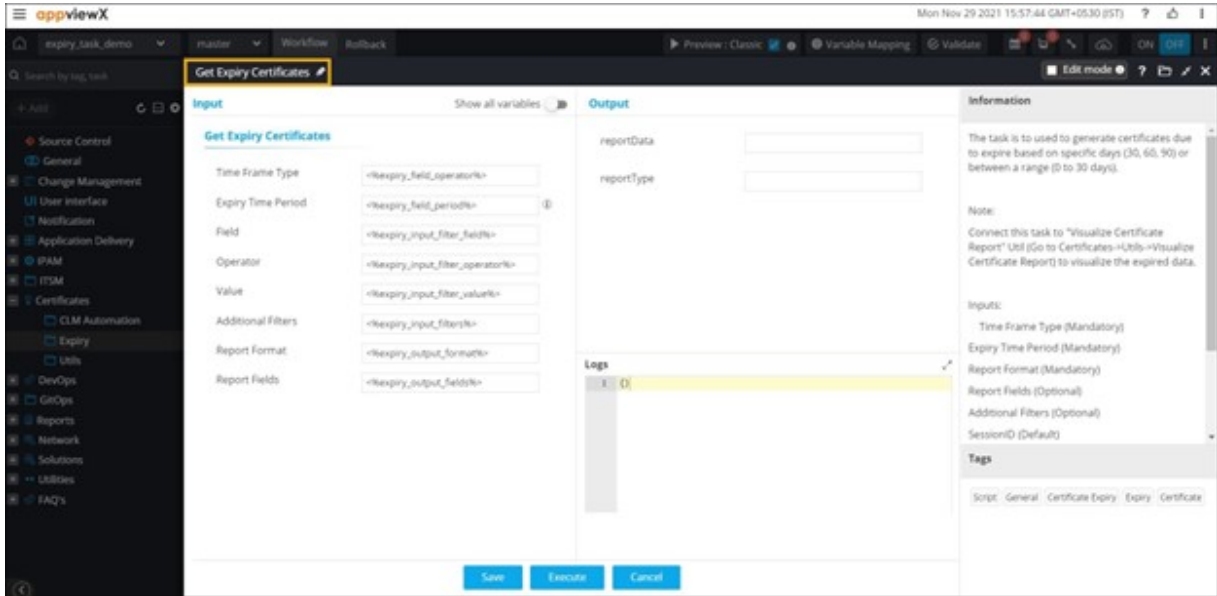
3. On the **Workflow** inventory page, click **Design**.
4. Enter a suitable **Name** for the workflow.
5. Click **Save**.



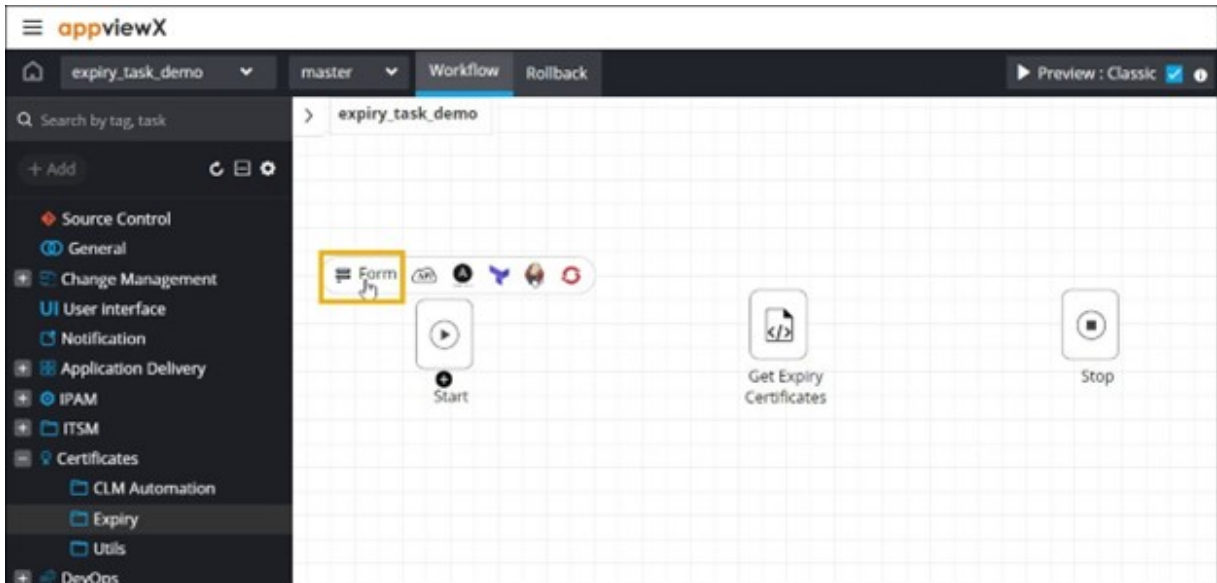
6. From the **Certificates** folder, under **Expiry**, drag and drop the **Get Expiry Certificates** task.



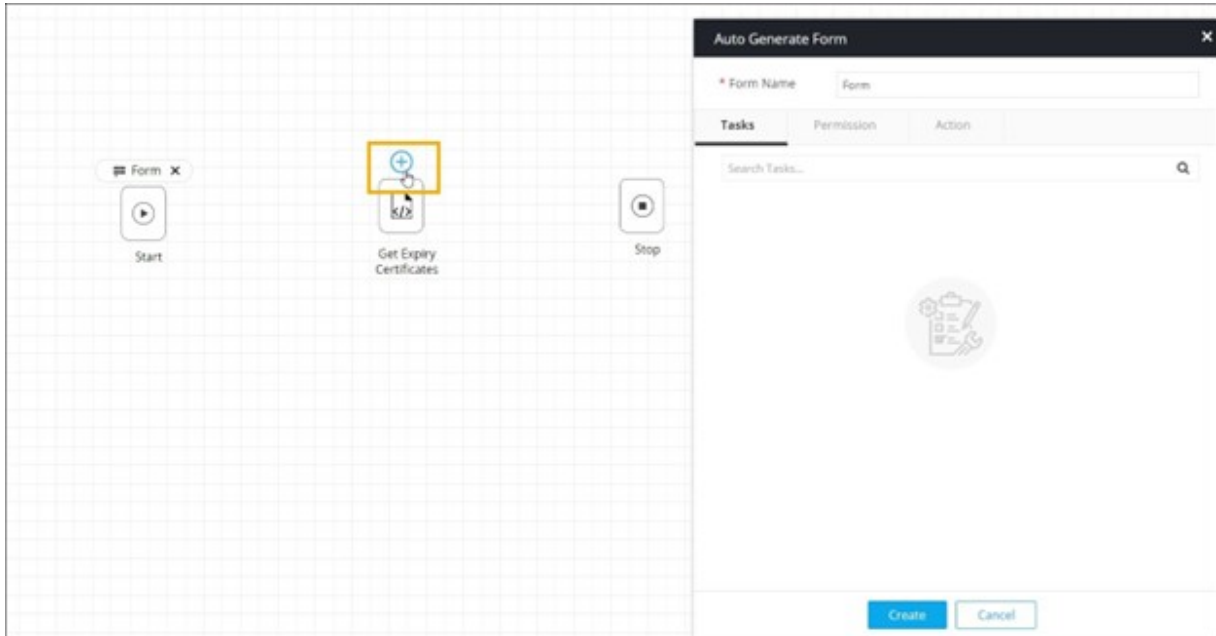
This task can be used to generate a report listing certificates due to expire in a specific number of days.



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

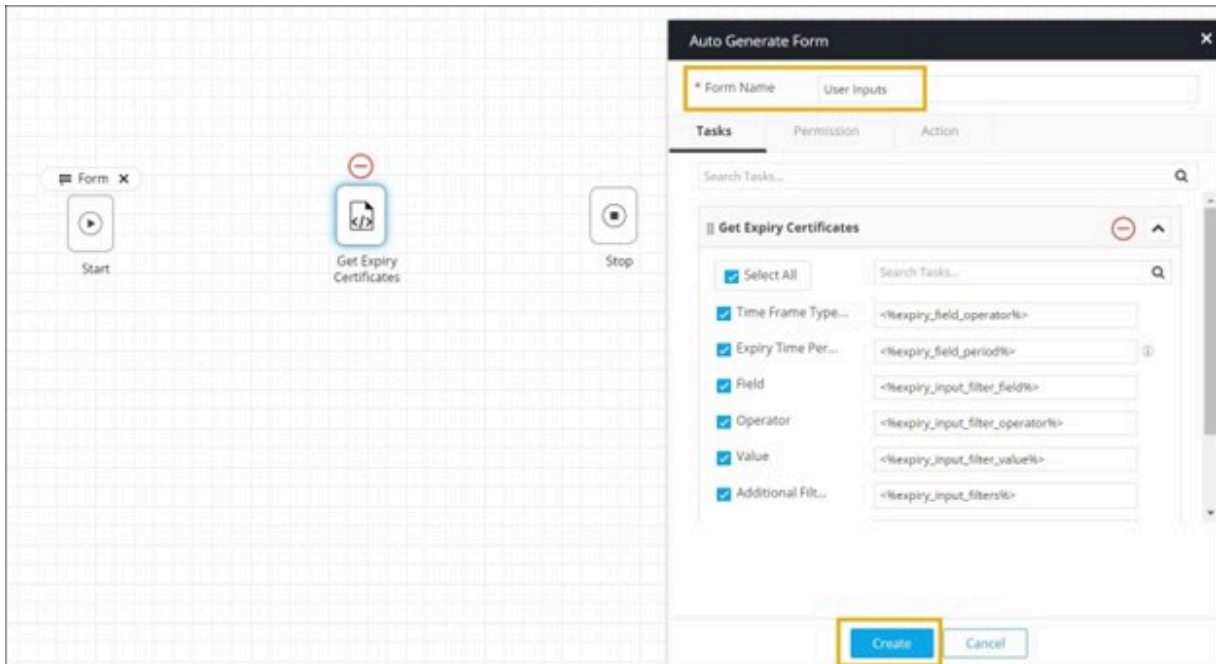


8. Click **+** above the **Get Expiry Certificates** task to auto-populate the form fields.

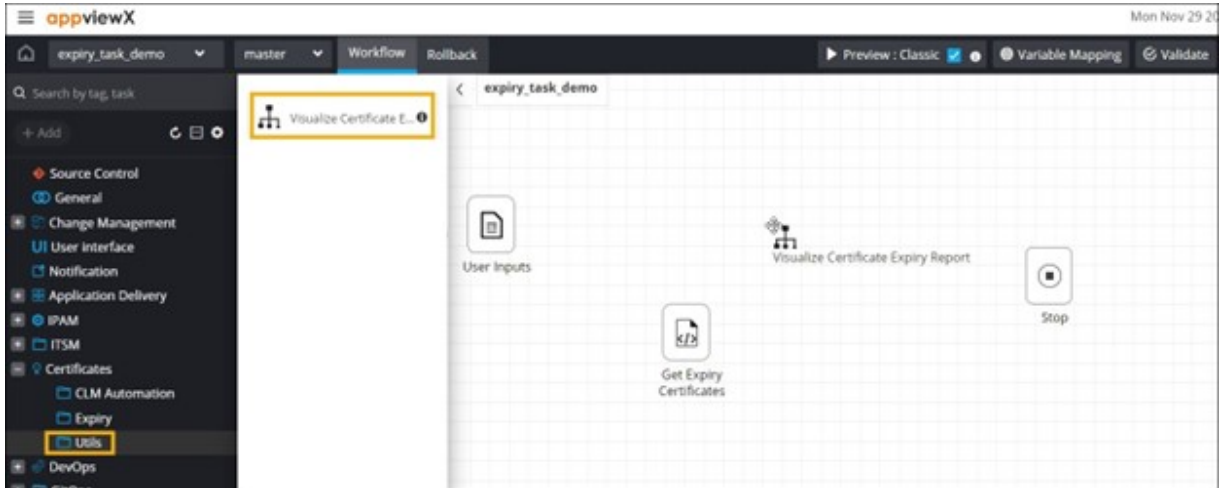


9. Select the fields required in the input form.

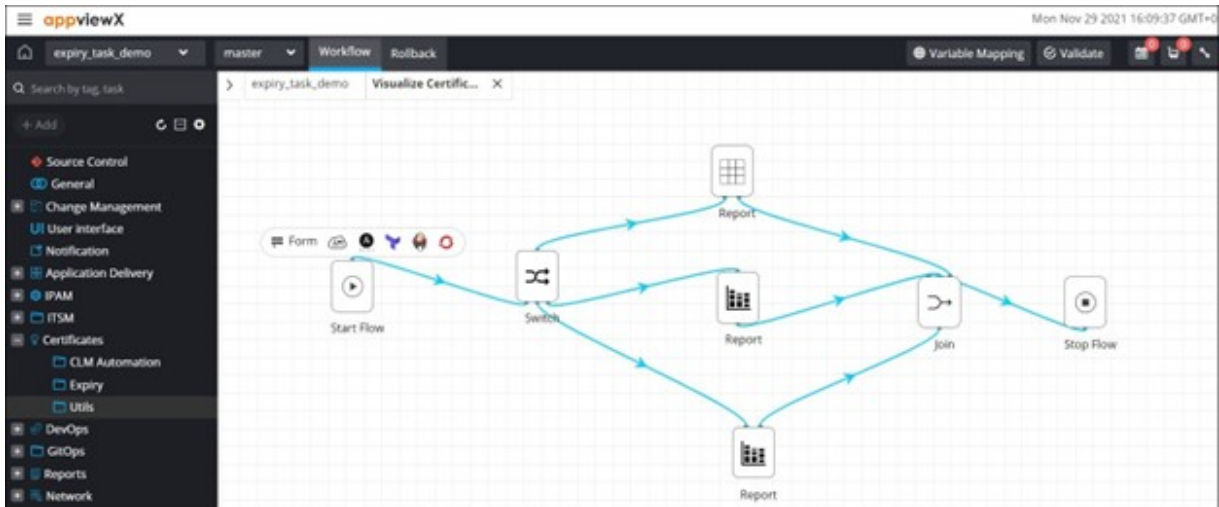
10. Provide a **Form Name** and click **Create**.



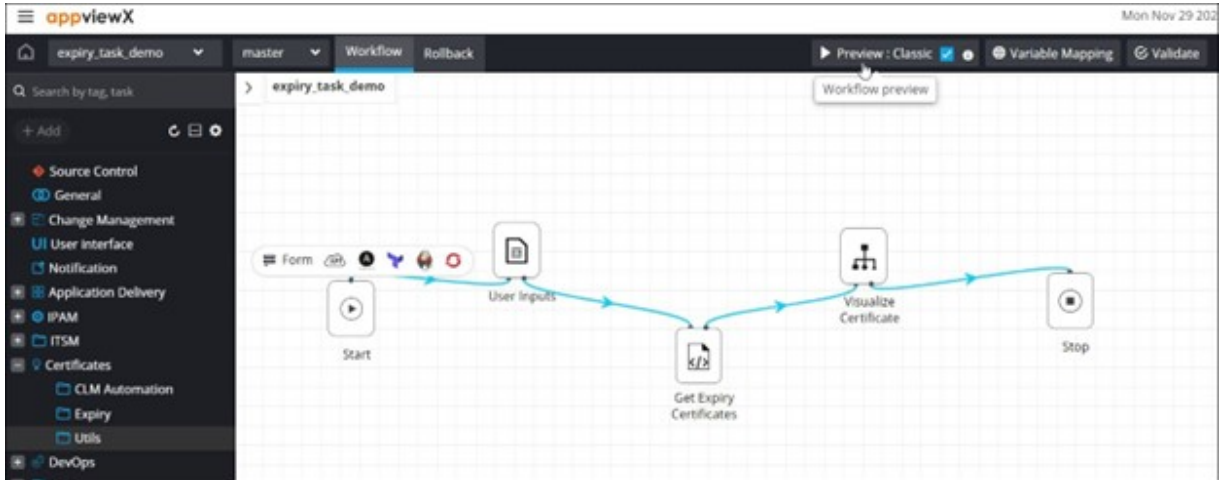
11. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.



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.



12. 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 the 'User Inputs' form for the 'Get Expiry Certificates' task. The form is titled 'Get Expiry Certificates' and has the following fields and options:




- Time Frame Type: Exact (dropdown)
- Expiry Time Period: (text input)
- Field: Type (dropdown)
- Operator: is (dropdown)
- Value: (text input)
- Additional Filters: (table with search, field, operator, value columns)
- Report Format: Default (dropdown)
- Report Fields: None Selected (dropdown)


Buttons at the bottom include 'Next', 'Save draft', and 'Cancel'.


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

Field	Description
Time Frame Type	Enter the time frame type from the available options: <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).

Field	Description
	 Note: Exact is the default selection.
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	Select the conditional operator: <ul style="list-style-type: none"> • Is • Is Not
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  Note: The steps to apply these additional filters are given below the table.
Report Format	Select the format in which the report is displayed from the available options: <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.

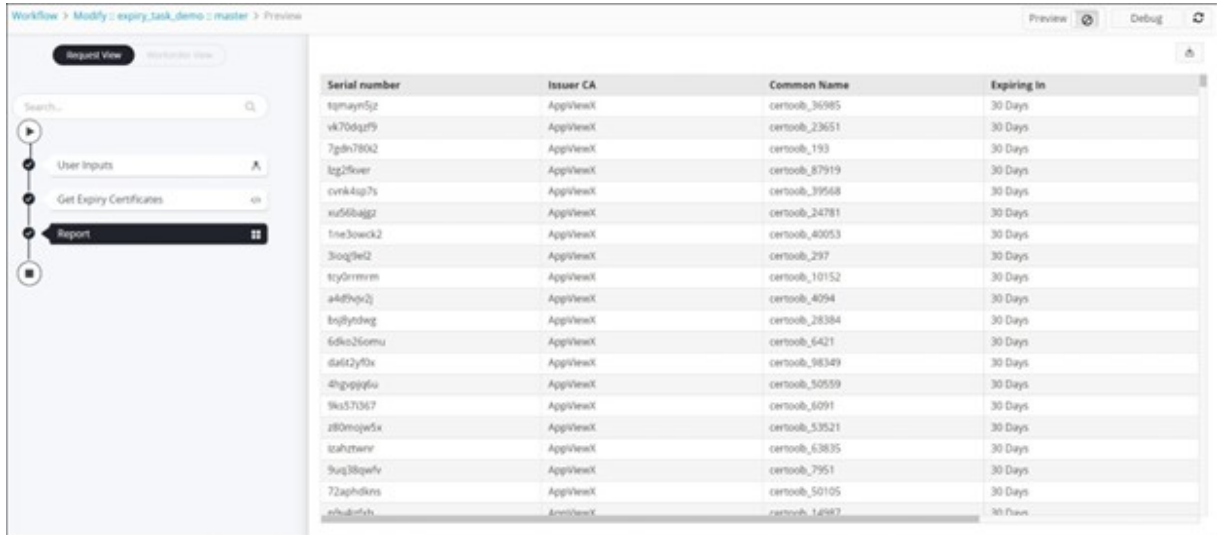
- To add filters to the **Additional Filters** grid, click .
- To edit the value of a particular filter, select the filter in the grid and click .
- Enter the new value(s) for the filters (Field/Operator/Value) and click  again to update the value(s).

16. To delete a filter, select the filter in the grid and click .

17. To maximize the **Additional Filters** grid, from the top right corner of the grid, click .

18. Click **Next**.

Report generated with expiry certificates data displayed in Grid format.



Serial number	Issuer CA	Common Name	Expiring In
tsmays5z	AppViewX	certool_36985	30 Days
vk70qz79	AppViewX	certool_23651	30 Days
7gdn7802	AppViewX	certool_193	30 Days
lzz2fseer	AppViewX	certool_87919	30 Days
cvnk4sp7s	AppViewX	certool_39568	30 Days
ku56baggz	AppViewX	certool_24781	30 Days
lne3owck2	AppViewX	certool_40053	30 Days
3ooq2e2	AppViewX	certool_297	30 Days
ty0rmrm	AppViewX	certool_10152	30 Days
a48hg-2j	AppViewX	certool_4094	30 Days
8qjlytdwg	AppViewX	certool_28384	30 Days
6dks26emu	AppViewX	certool_6421	30 Days
daf42yfdx	AppViewX	certool_98349	30 Days
4hgppjfu	AppViewX	certool_50559	30 Days
9ks57l367	AppViewX	certool_6091	30 Days
z80mow5x	AppViewX	certool_53521	30 Days
icpfzterr	AppViewX	certool_63835	30 Days
9ug38qwfV	AppViewX	certool_7951	30 Days
72ap4dkns	AppViewX	certool_50105	30 Days
ehubofyh	AppViewX	certool_14987	30 Days



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

Chapter 6: 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.