appviewX

CERT+ Automation Workflows User Guide

Version: 2021.1.0

Copyright AppViewX, Inc.

Trademarks

External Reference Links

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

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

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

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for whichyou supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text thatappears on the screen, or text that you enter.

Chapter 1: Prerequisites

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

Web Browser Requirement

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

Chapter 2: Role-Based Access Control

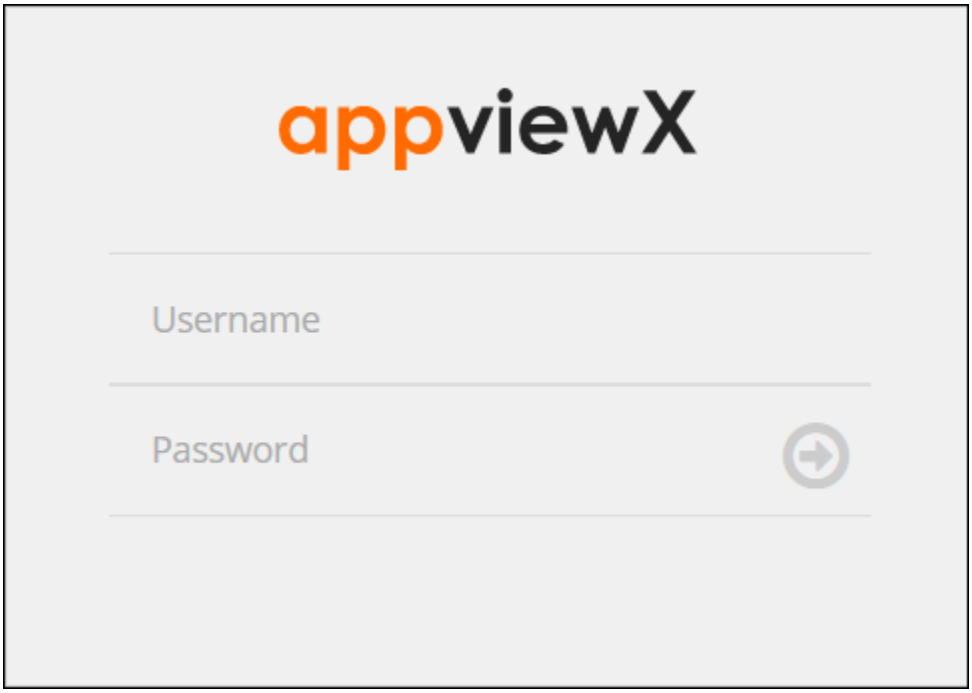
With role-based access control (RBAC), you can assign permissions to users for accessing the module and allow/restrict them to perform certain actions. You can refer to this link and find out more about RBAC.

Chapter 3: Accessing CERT+ Automation Workflows

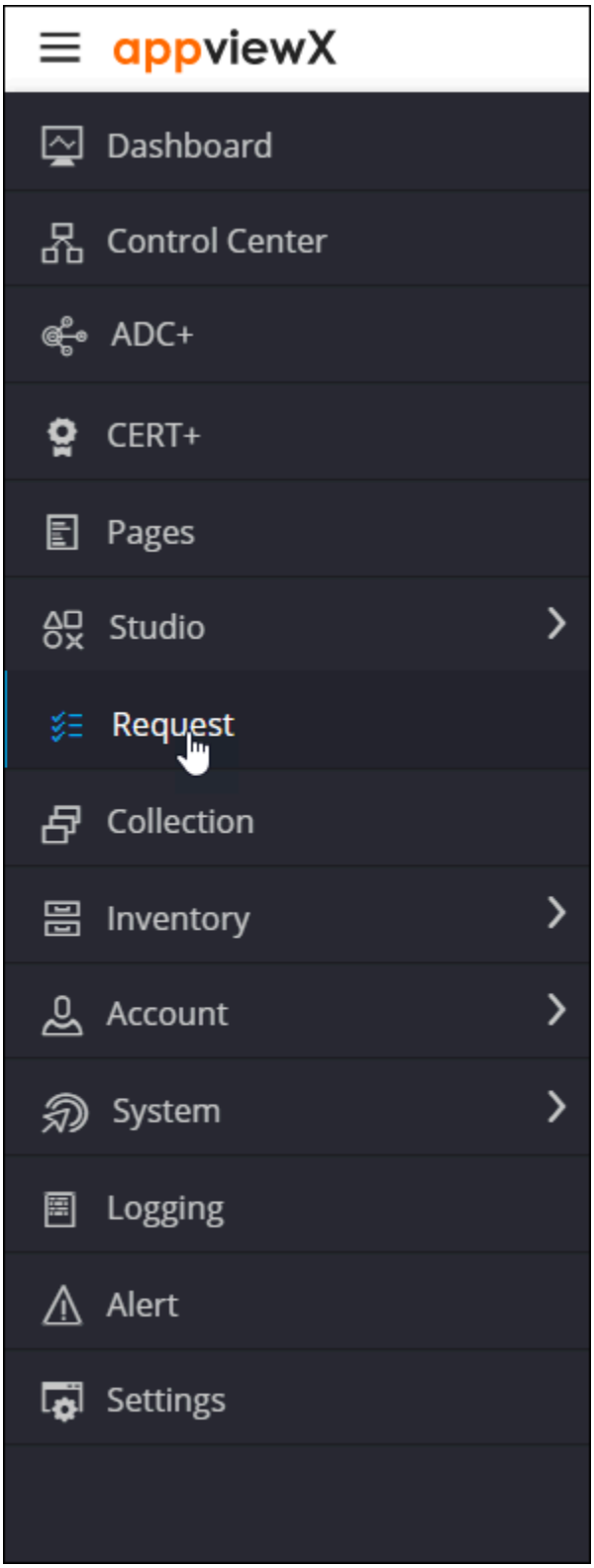
The CERT+ Automation workflows are available on the Workflow **Catalog** page.

To view these workflows:

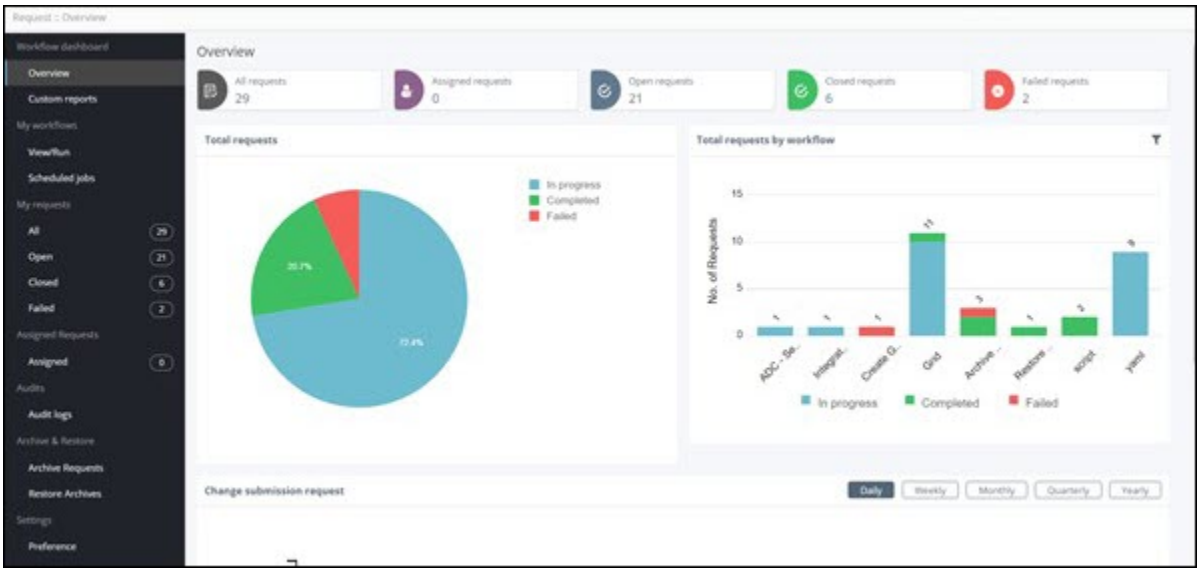
1. Log into AppViewX with valid credentials.



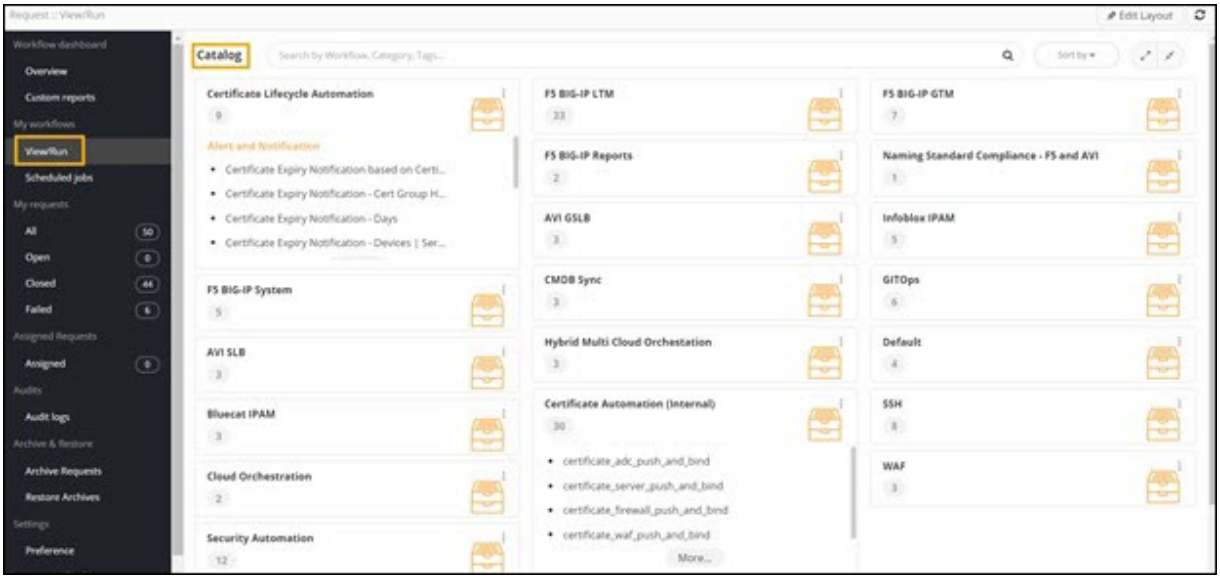
2. To access the navigation pane, hover the mouse over ☰.
3. From the menu displayed, click **Request**.



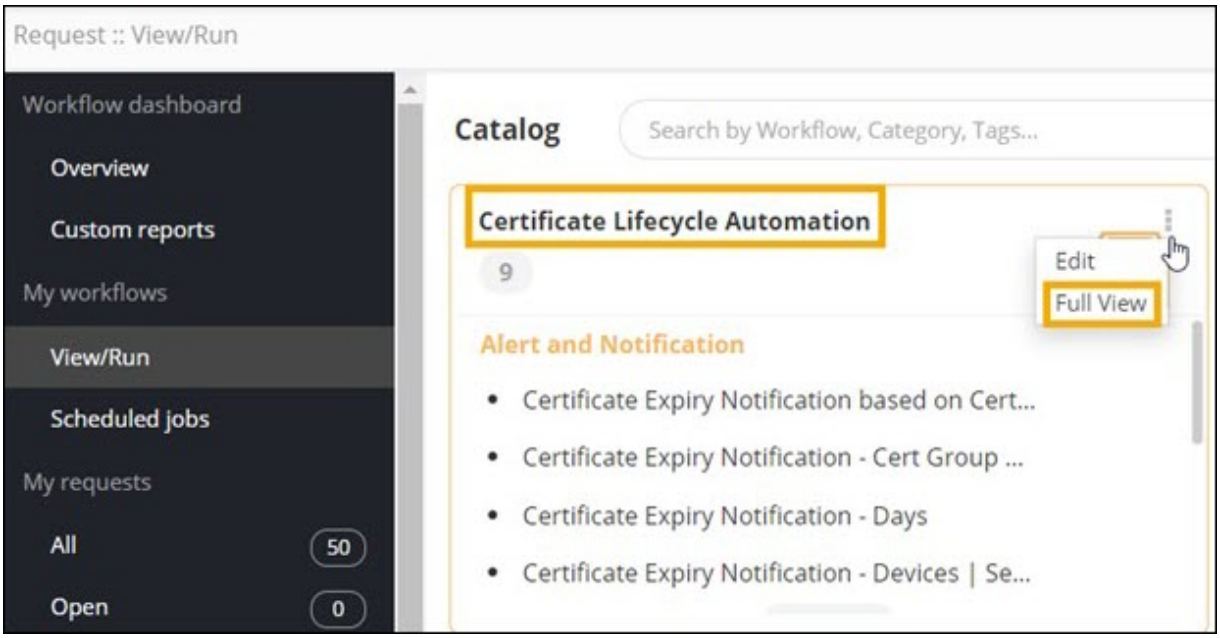
The Workflow **Request** page is displayed, with the **Overview** section open by default.



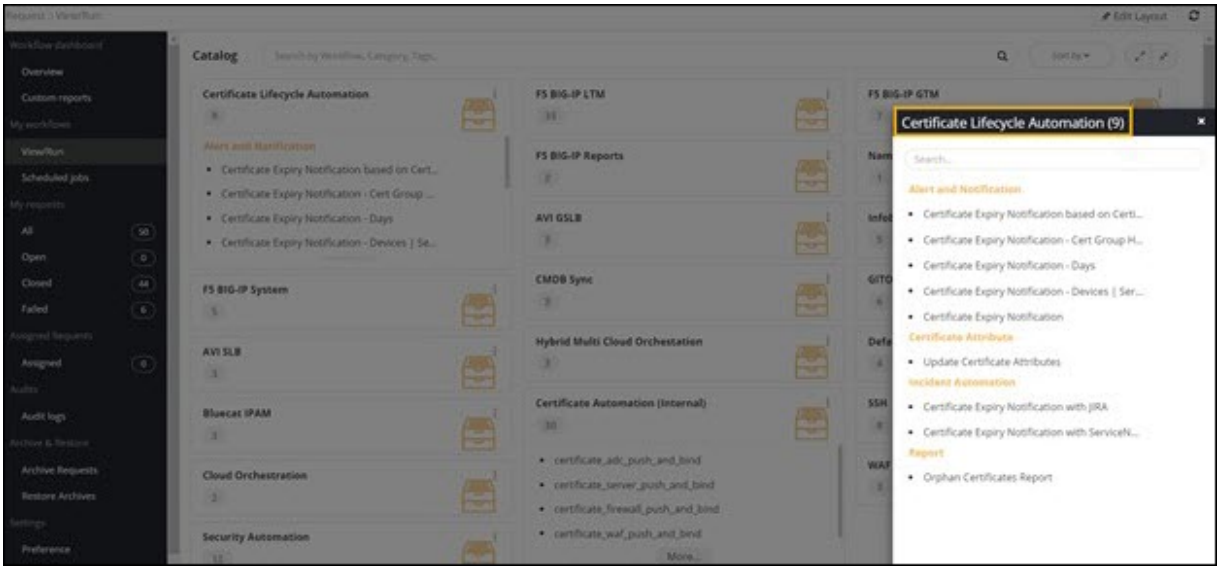
4. On the Workflow **Request** page, from the navigation menu on the left, select **View/Run**.
   The workflow **Catalog** page is displayed.



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



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



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

Chapter 4: Certificate Expiry Workflows

Overview

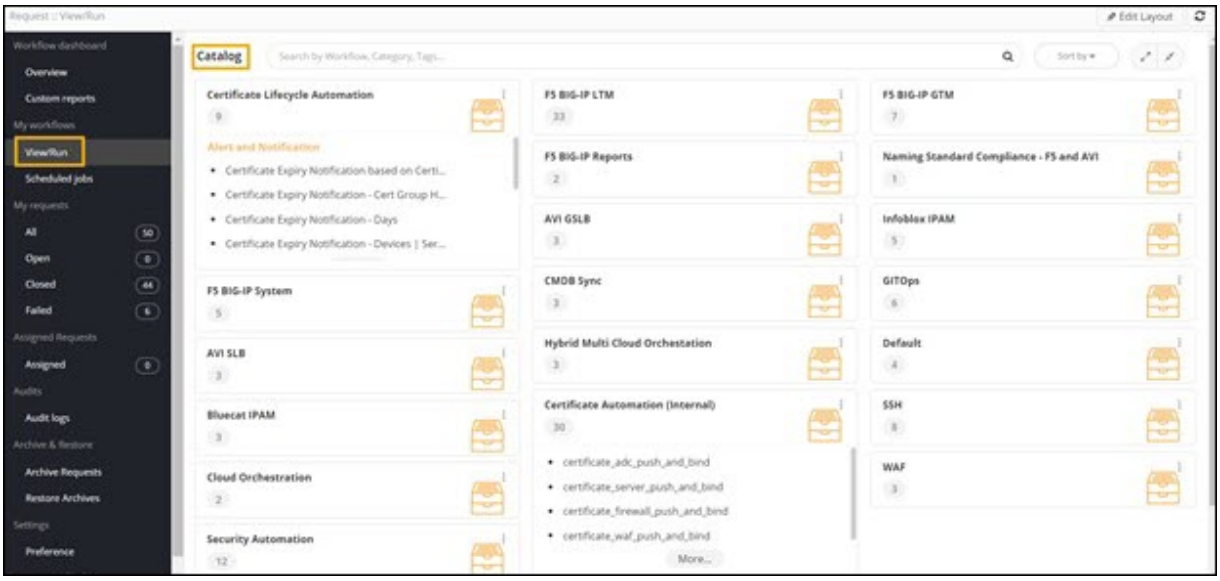
This section lists and describes the workflows that can be used to notify the user(s) about the expiry of the certificates based on different criteria such as certificate attributes, expiry period, hierarchy, and so on. It also enables you to create tickets for expiring certificates on Jira/ServiceNow.

Certificate Expiry Notification based on Certificate Attributes

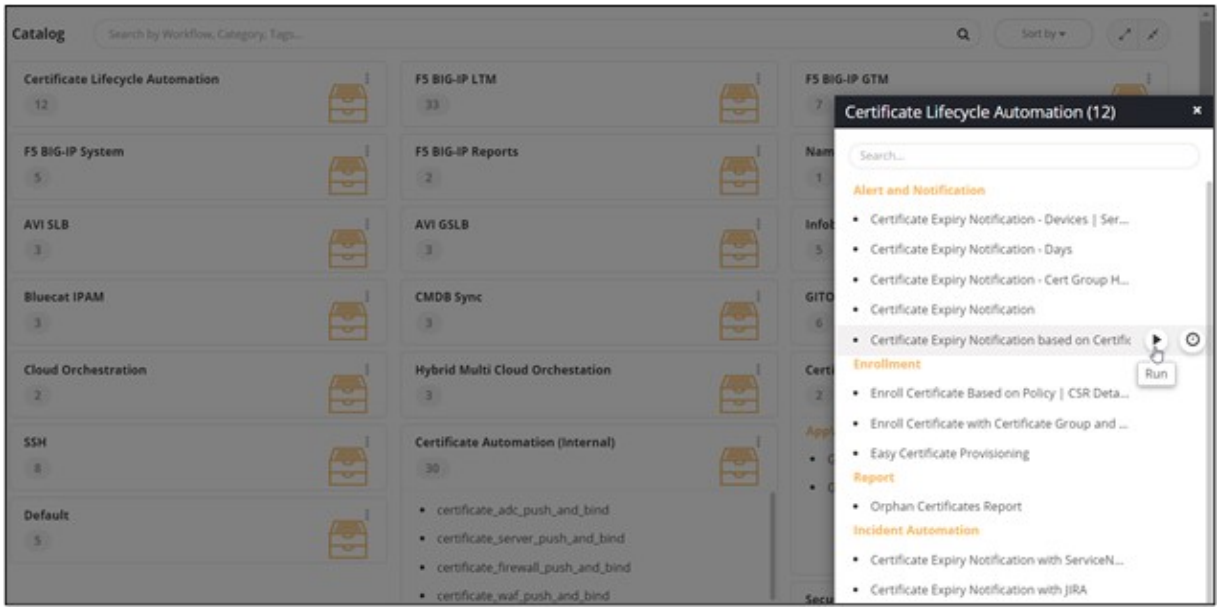
This workflow allows you to send an email notification listing certificates expiring in a specific number of days with selected certificate attribute details displayed in the email.

To trigger this workflow:

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

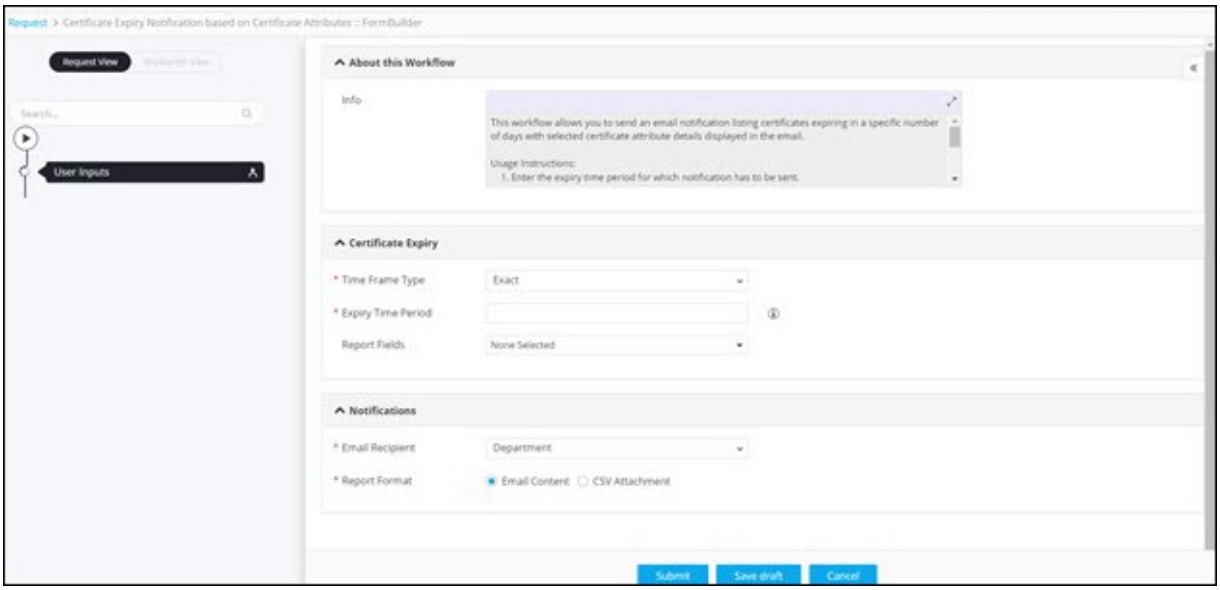


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

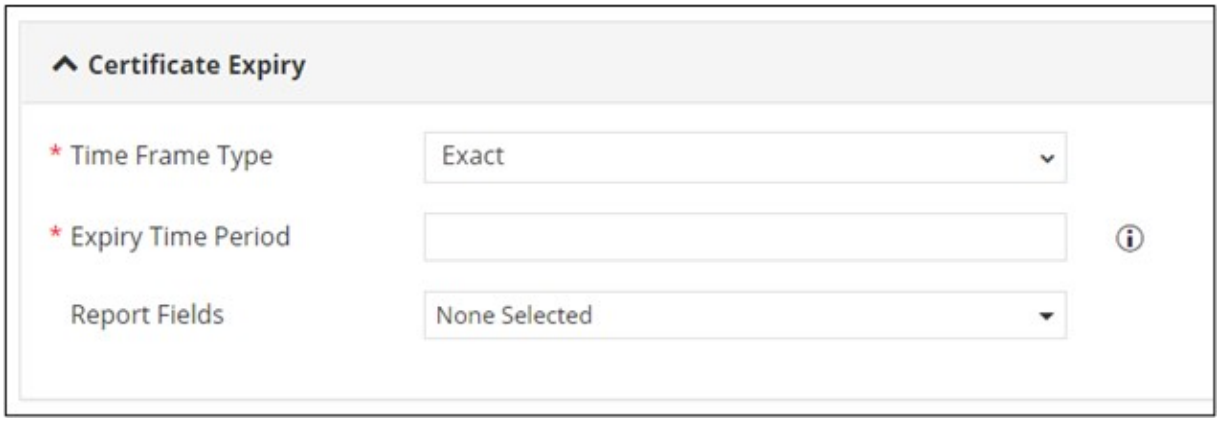


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



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

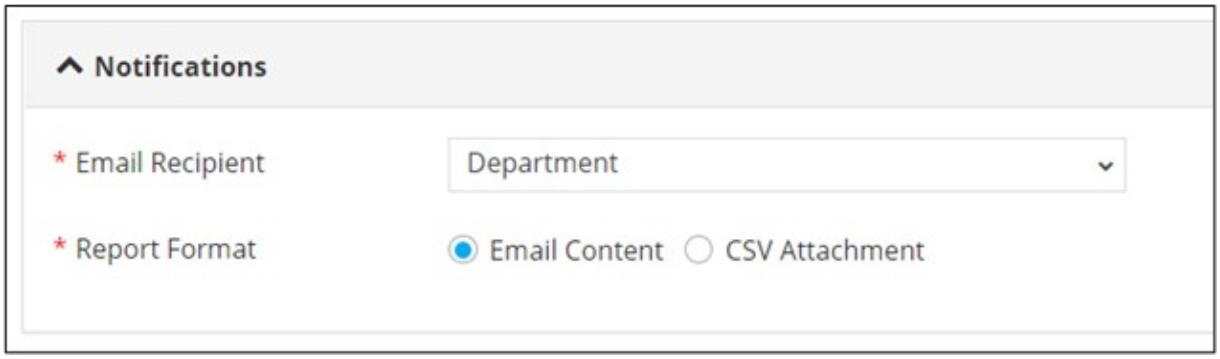


The following table describes the fields under the **Certificate Expiry** section:

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

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

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

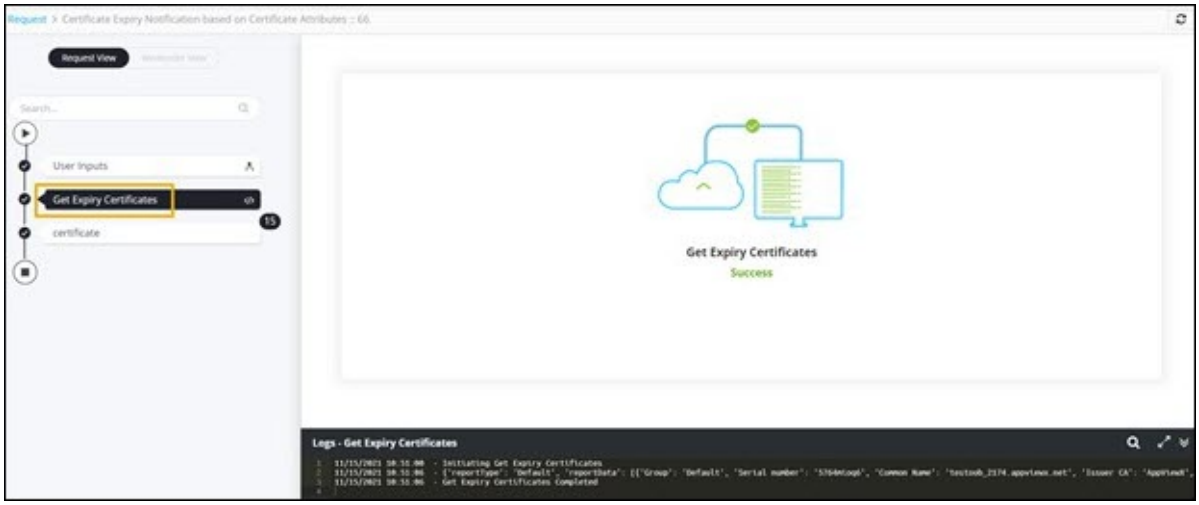


The following table describes the fields under the **Notifications** section:

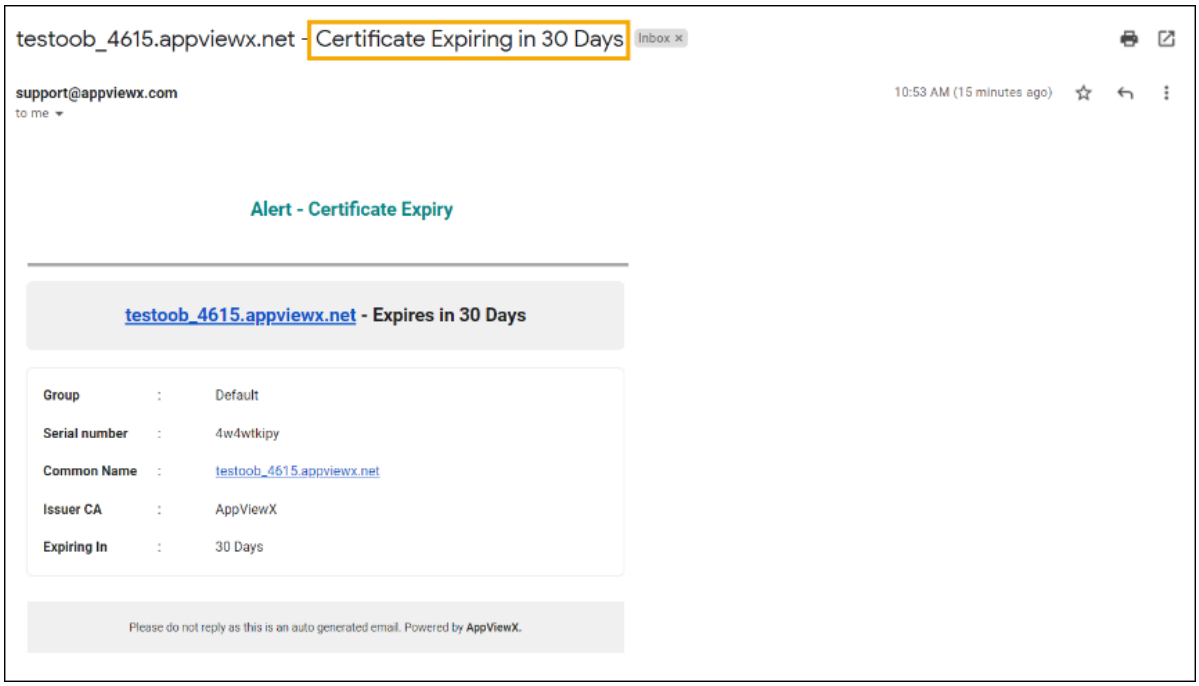
Field	Description
***Email Recipient**	Select the email recipient from the dropdown list.
***Report Format**	Select the required checkbox to send the report as: • **Email content** - The report will be sent as Email content. or • **CSV Attachment** - The report will be sent as a separate attachment in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

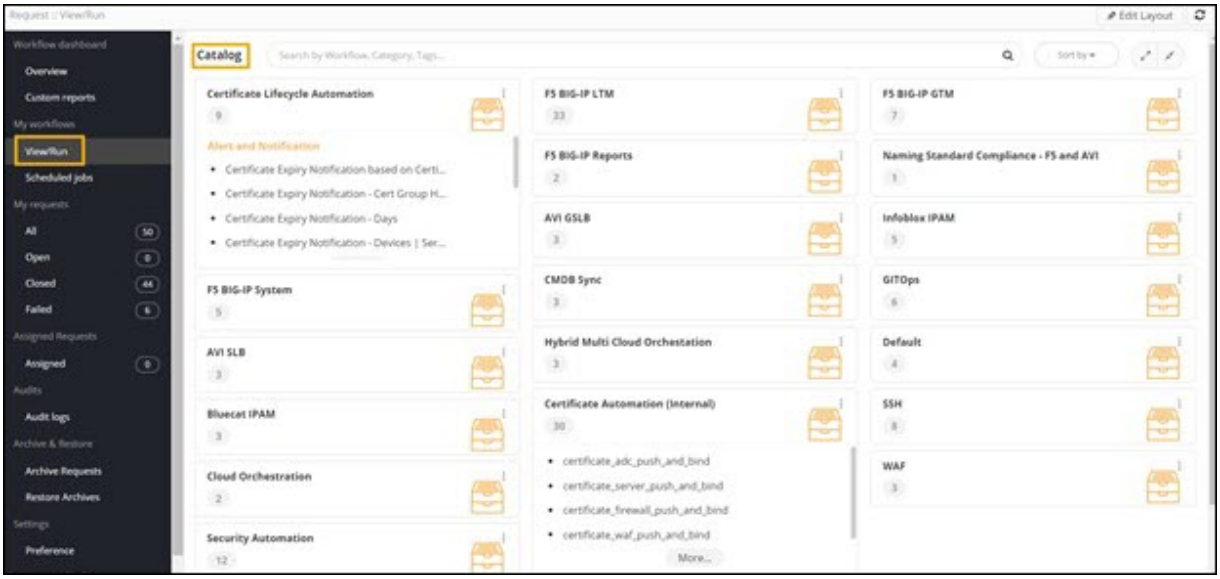


Certificate Expiry Notification - Cert Group Hierarchy

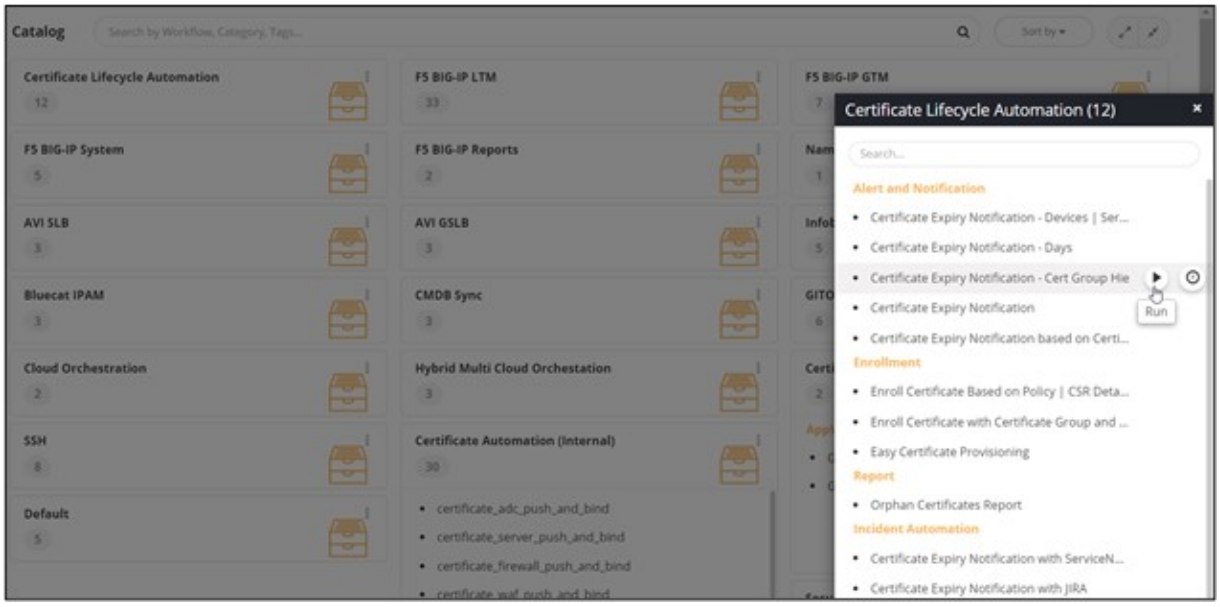
This workflow allows you to send a certificate expiry report notification to the certificate group and its associated hierarchical groups.

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.

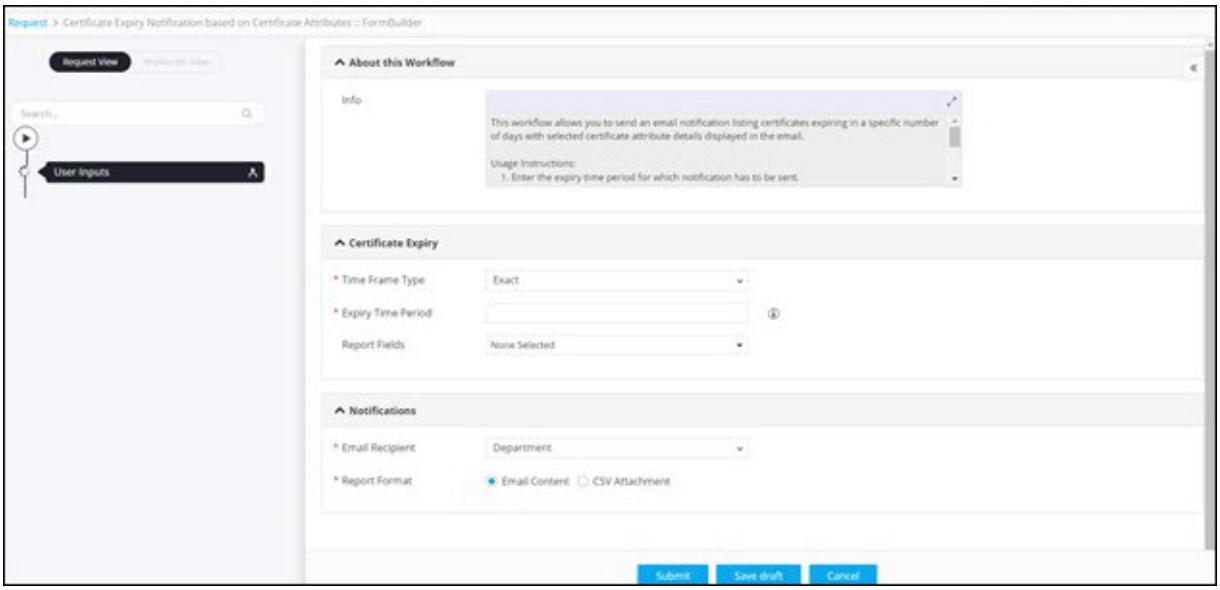


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

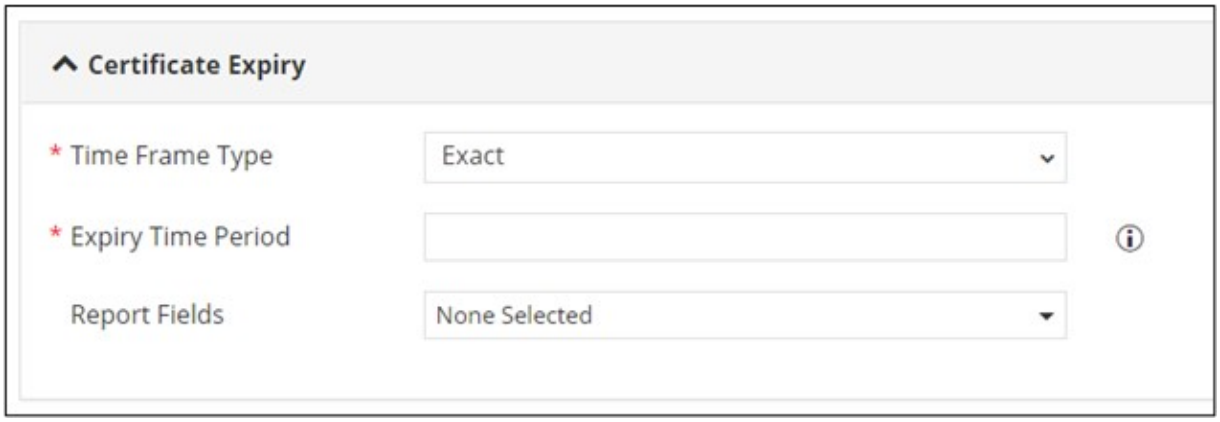


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



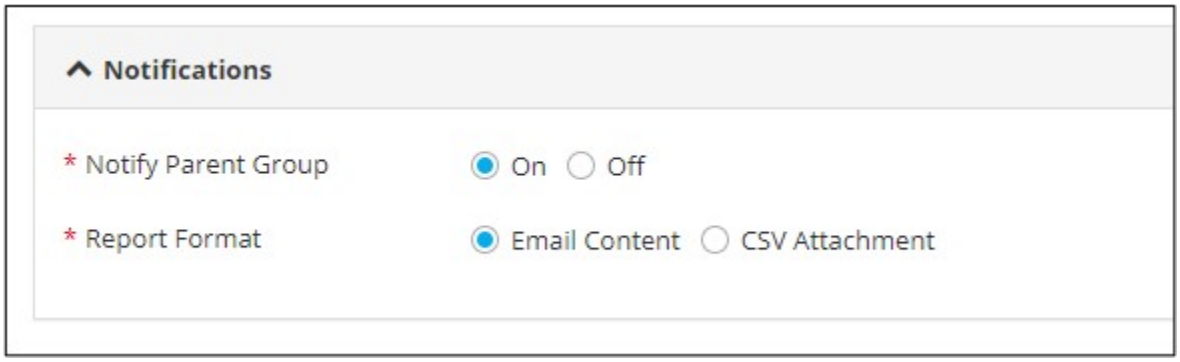
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



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

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

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



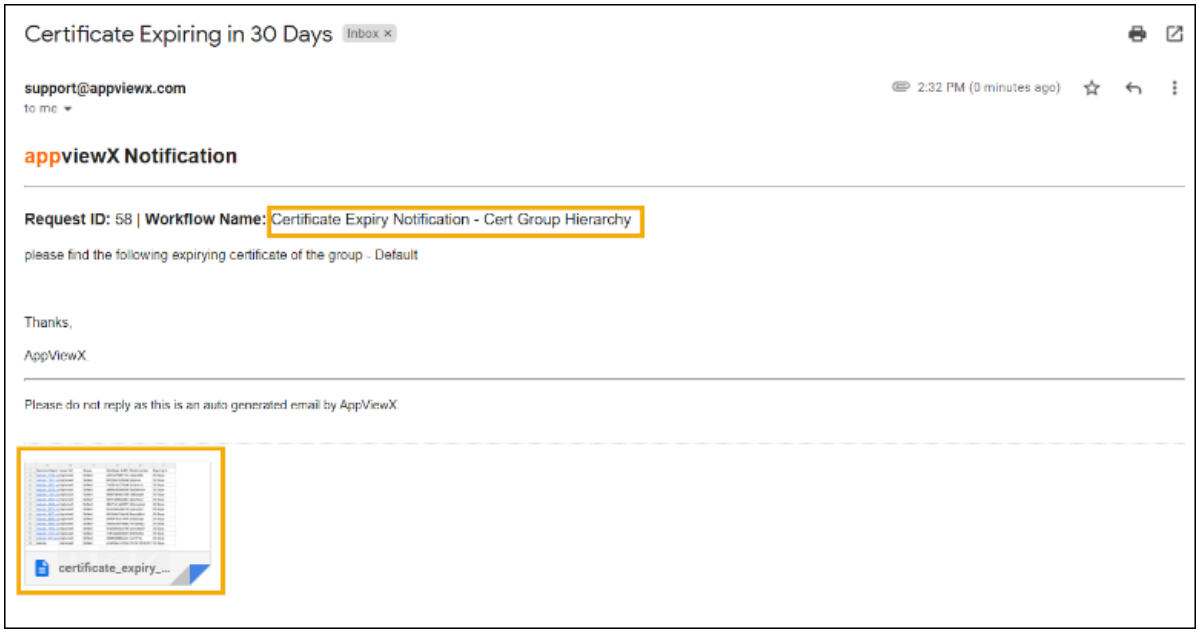
The following table describes the fields under the **Notifications** section:

Field	Description
***Notify Parent Group**	Select **On** if a notification has to be sent to the parent group of the certificate group. Select **Off** if a notification is not required to be sent to the parent group of the certificate group. **Note: On** is the default selection.
***Report Format**	Select the required checkbox to send the report as: • **Email content** - The report will be sent as Email content. or • **CSV Attachment** - The report will be sent as a separate attachment in CSV format. **Note: Email Content** is the default selection.
All Asterisk (*) marked fields are mandatory.	

7. Click **Submit**.

- **Get Expiry Certificates** task completed.

- Email notification received.

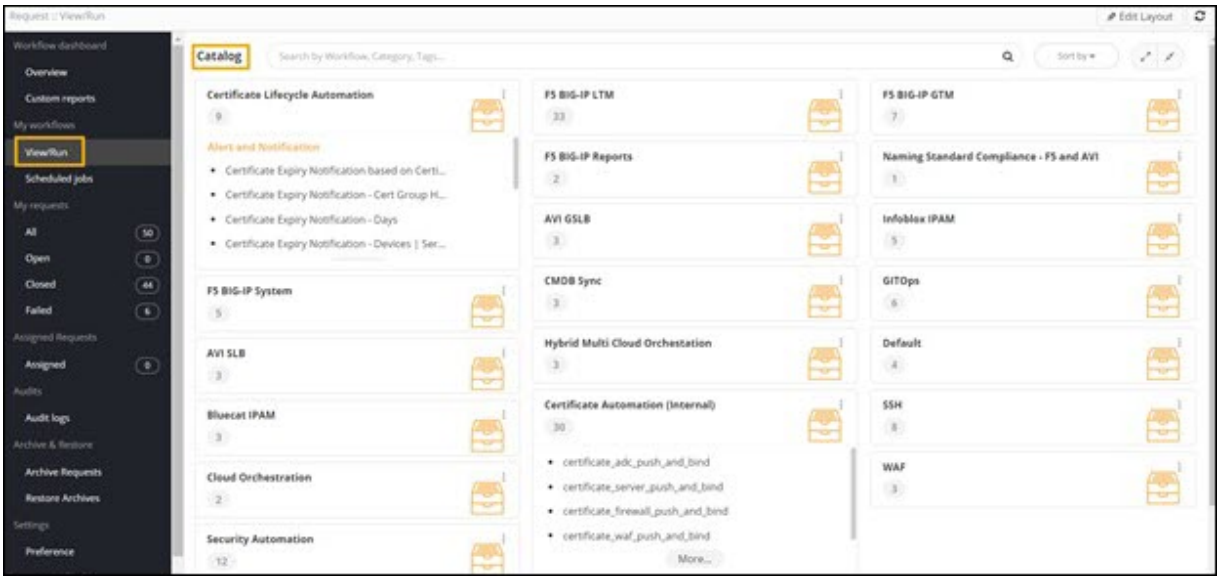


Certificate Expiry Notification - Days

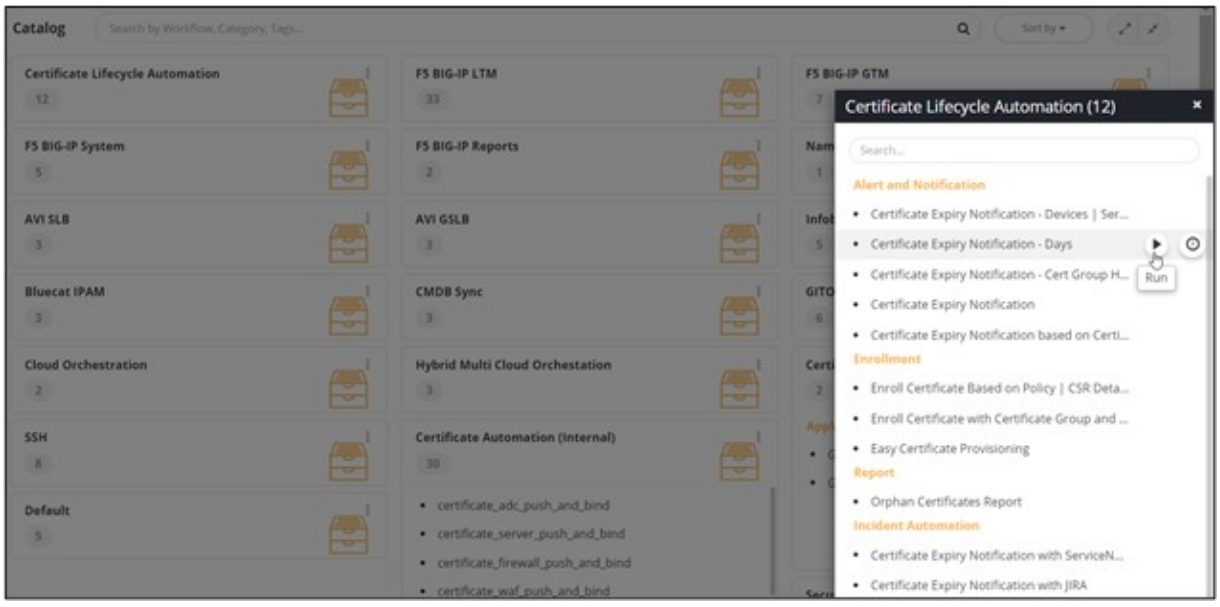
This workflow enables you to generate a report listing certificates expiring in a specific number of days to the email addresses present in the certificate or certificate group.

To trigger this workflow:

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

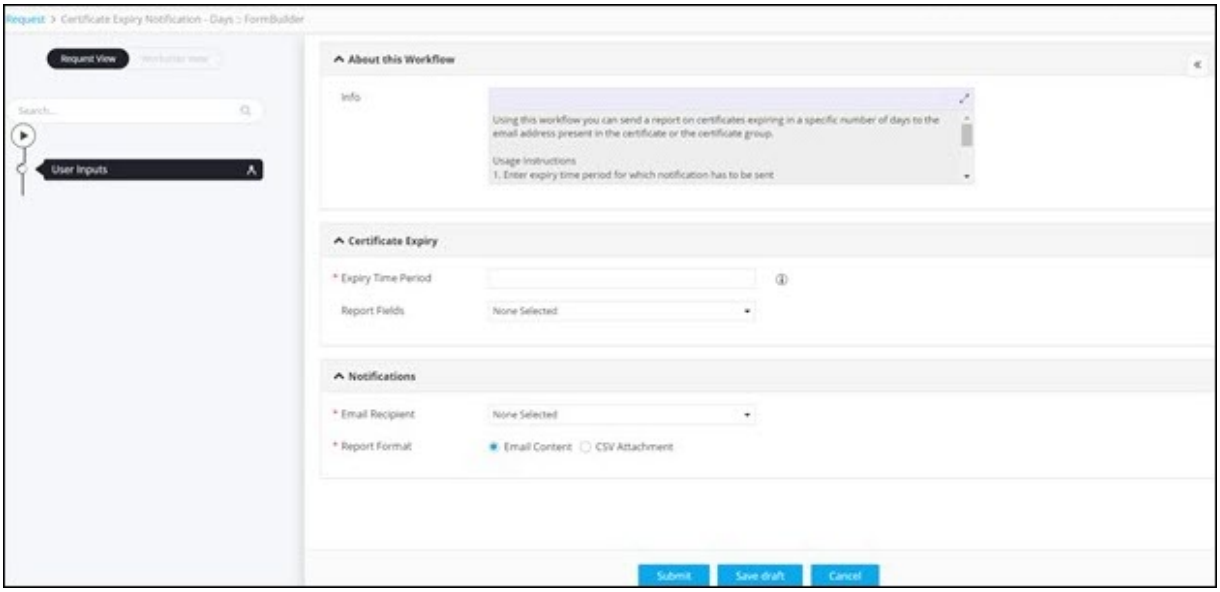


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

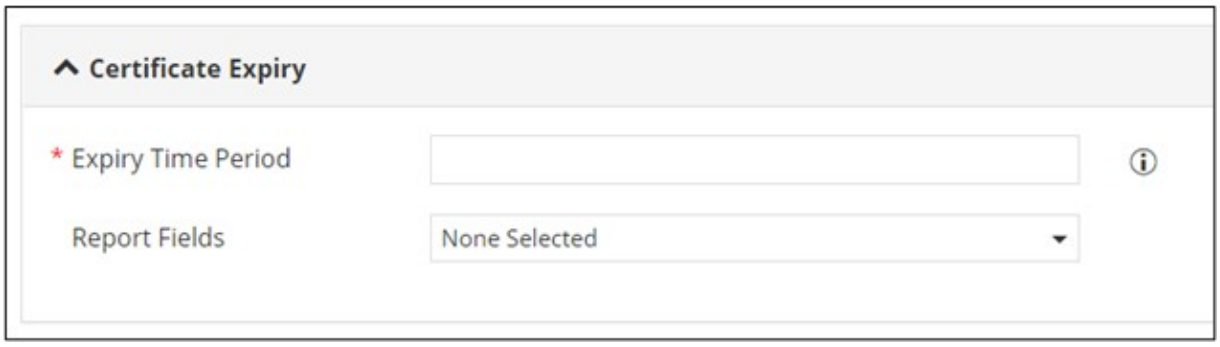


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



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

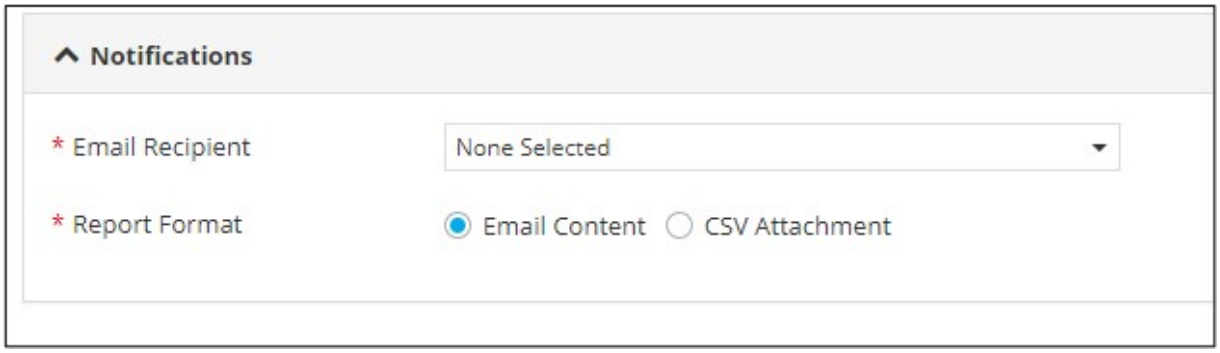


The following table describes the fields under the **Certificate Expiry** section:

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

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.

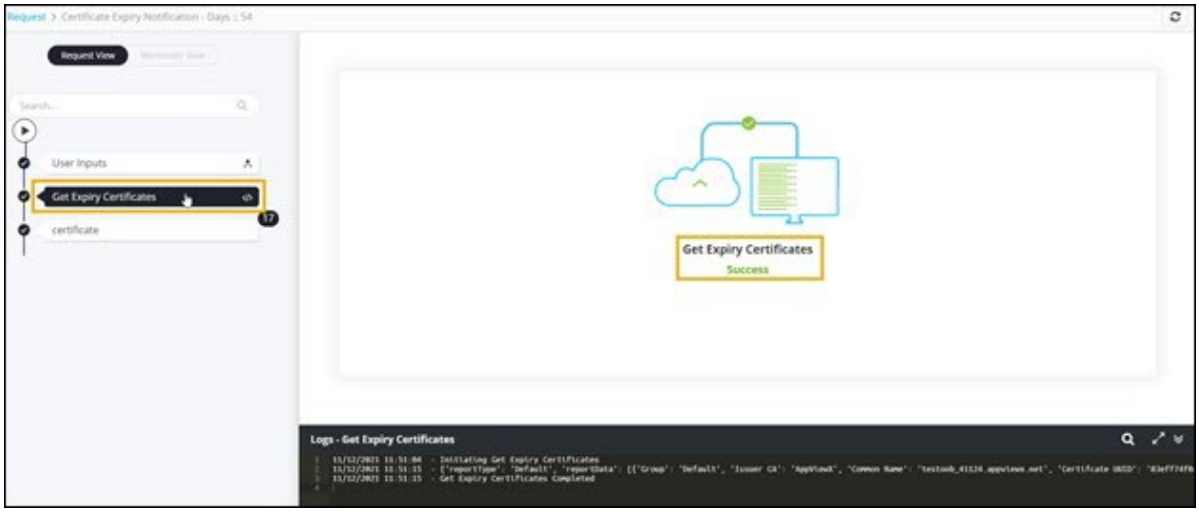


The following table describes the fields under the **Notifications** section:

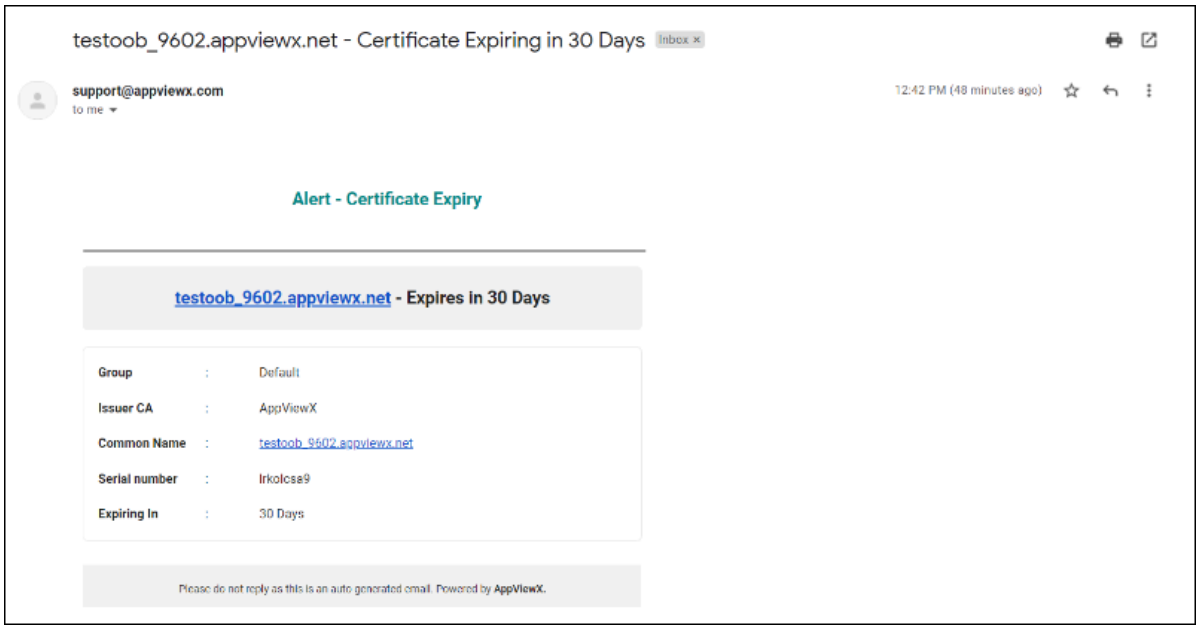
Field	Description
***Email Recipient**	Select the required recipient of the notification. You can select: • **Select all** • **Certificate Email -** The notification will be sent to the email addresses associated with the certificate. • **Certificate Group Email -** The notification will be sent to the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

7. Click **Submit**.

- Get Expiry Certificates task completed.



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

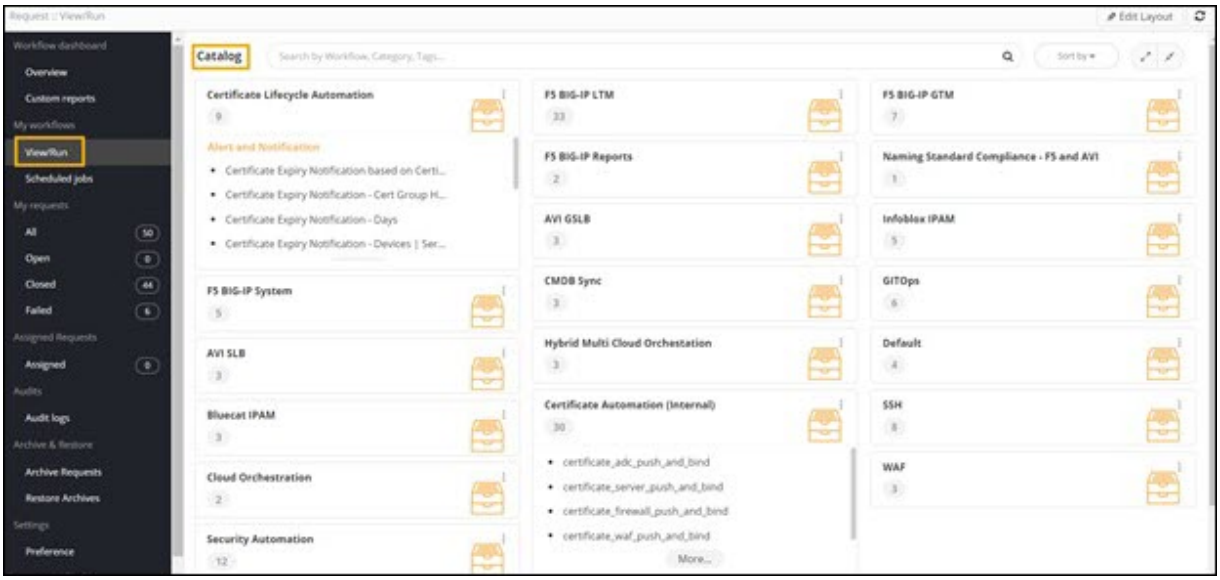


Certificate Expiry Notification - Devices | Servers

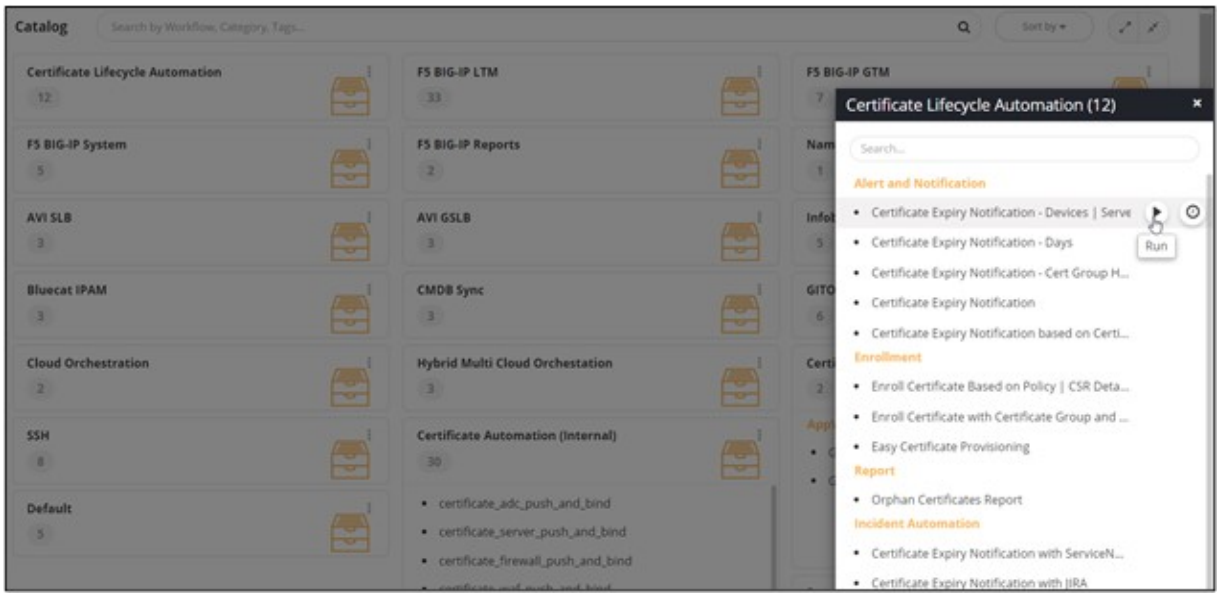
This workflow enables you to generate an expiry report of certificates present on a device and expiring in a specific number of days.

To trigger this workflow:

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

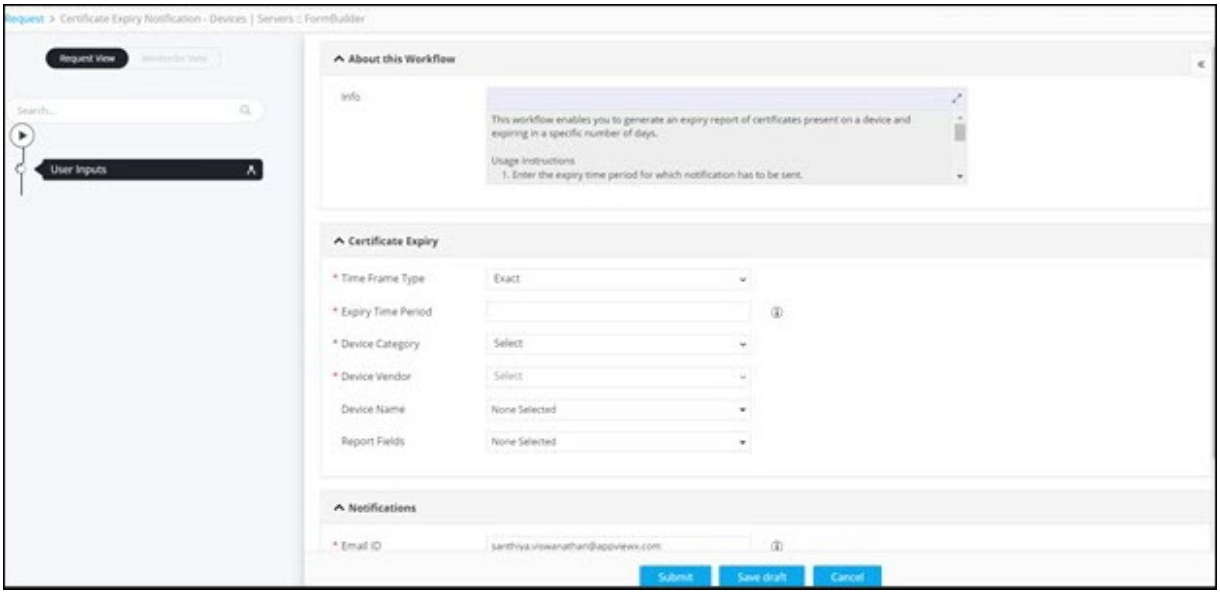


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification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

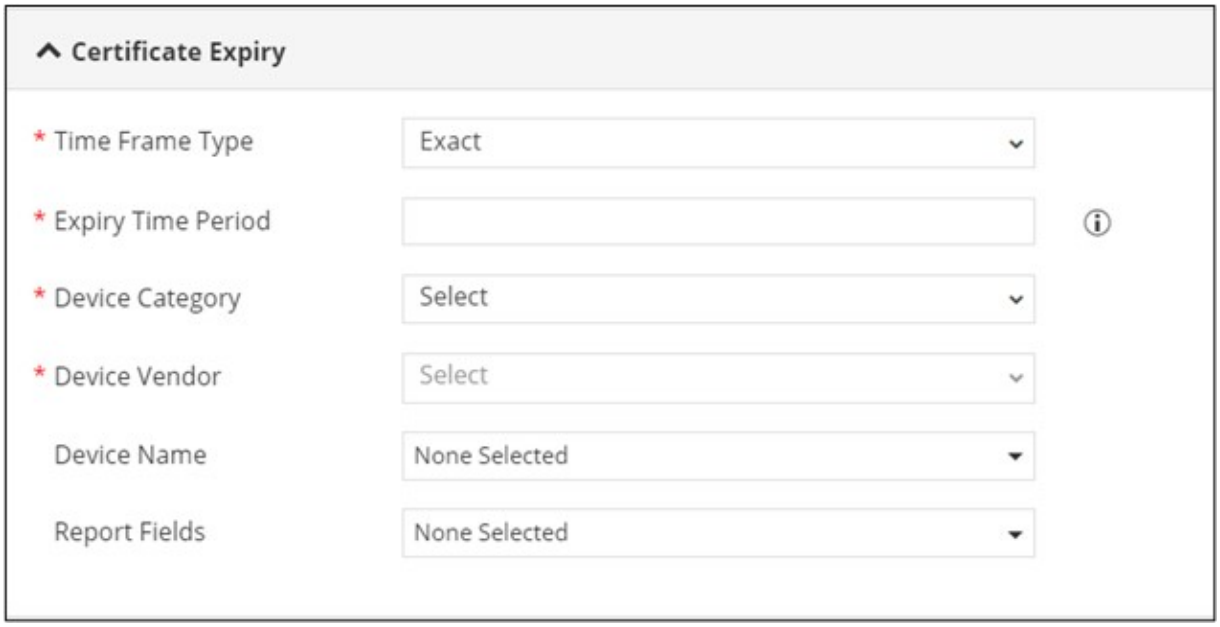


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



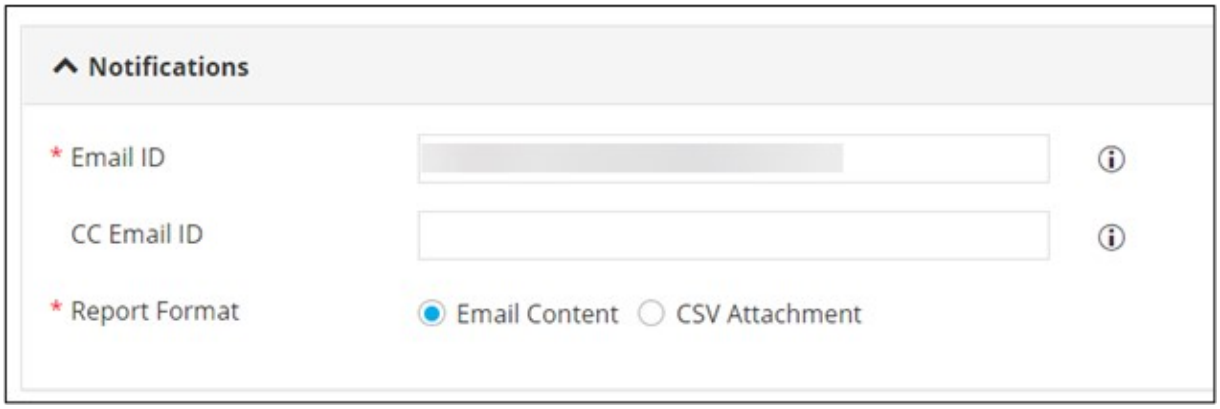
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



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

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

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

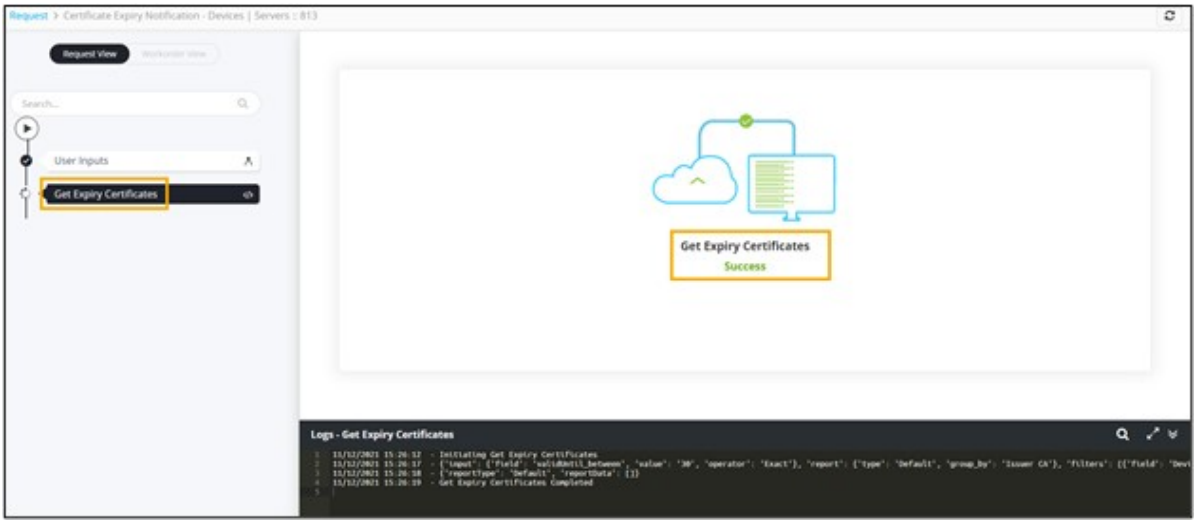


The following table describes the fields in the **Notifications** section:

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

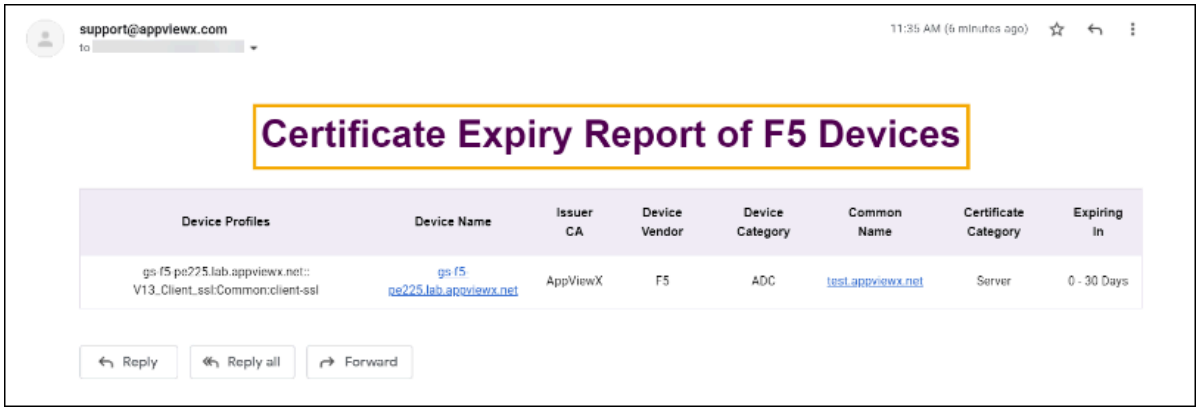
7. Click **Submit**.

- **Get Expiry Certificates** task completed.



- Certificate Device list generated.

• Email report received.

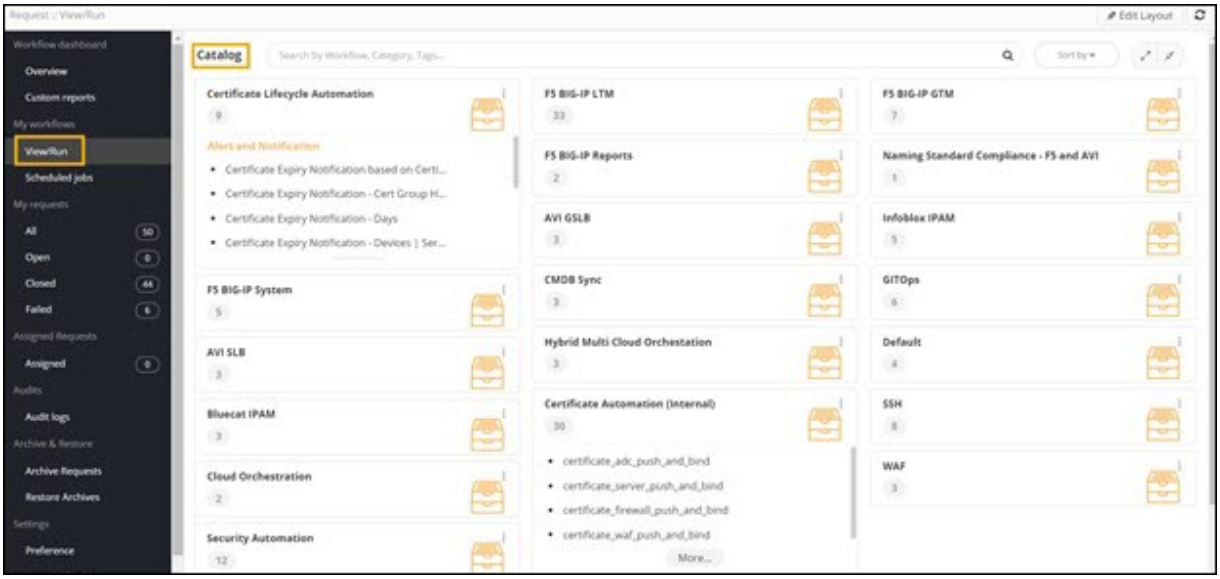


Certificate Expiry Notification

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

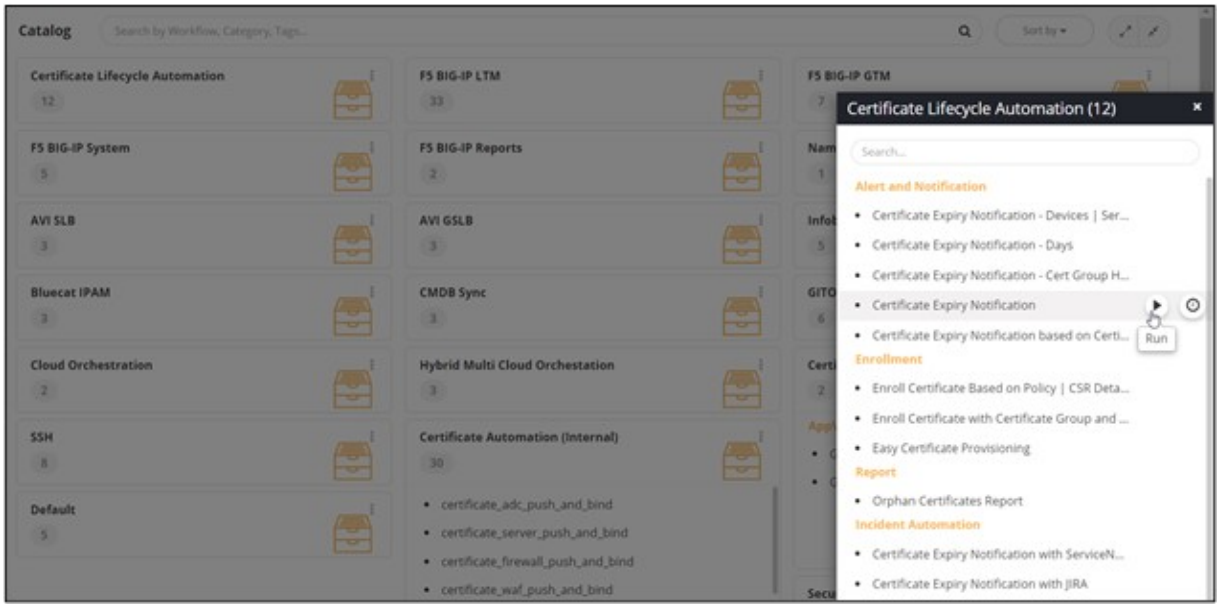
To trigger this workflow:

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



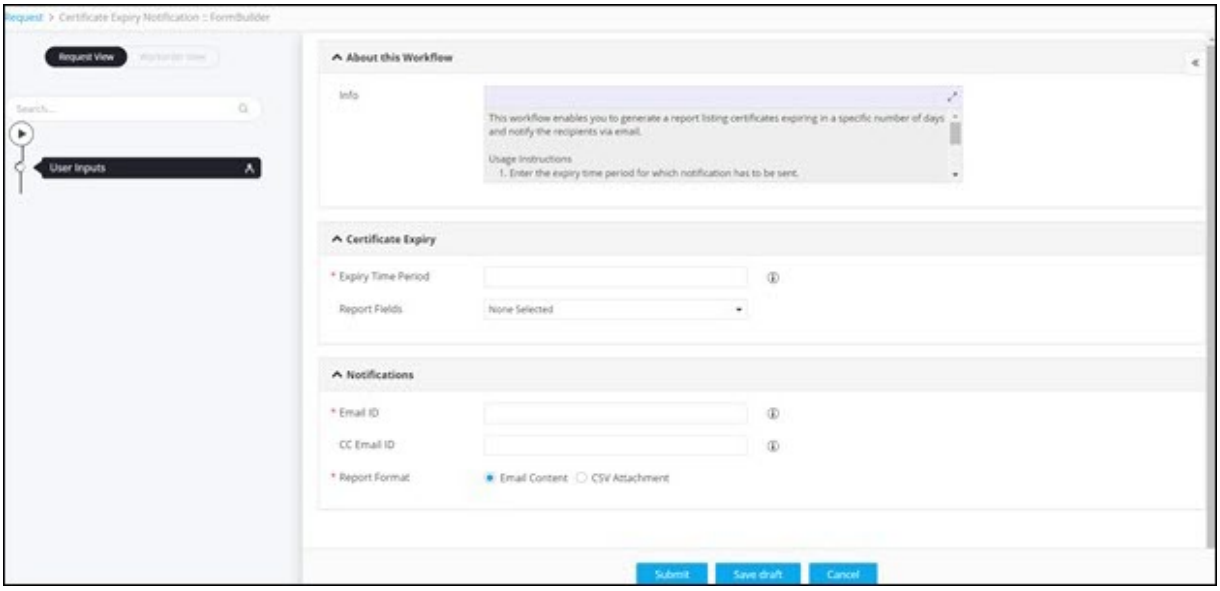
2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.

4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Certificate Expiry Notification** workflow and click  .

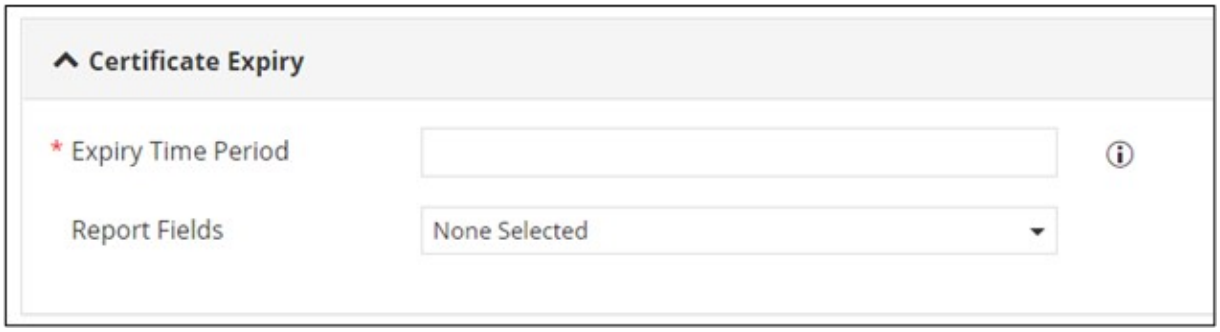


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



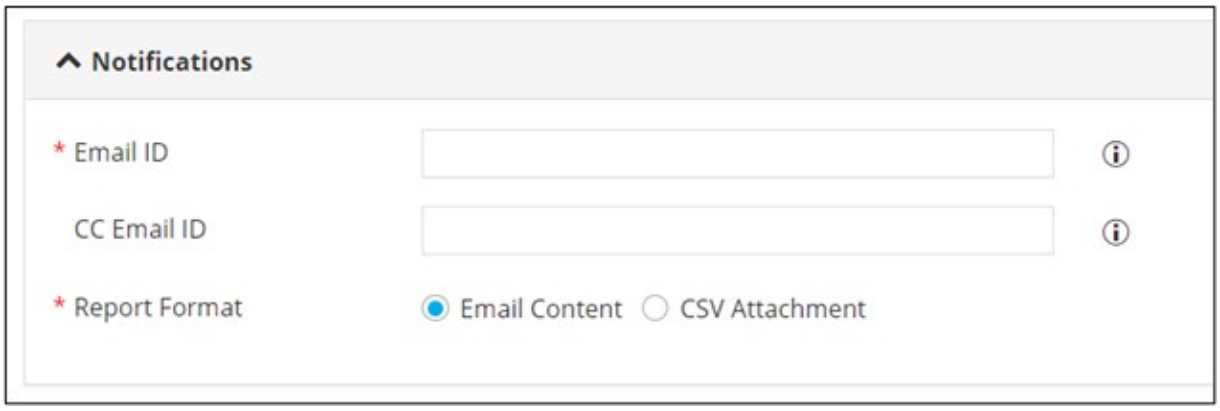
5. Under the **Certificate Expiry** section, enter or select the field information as shown.



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

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

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

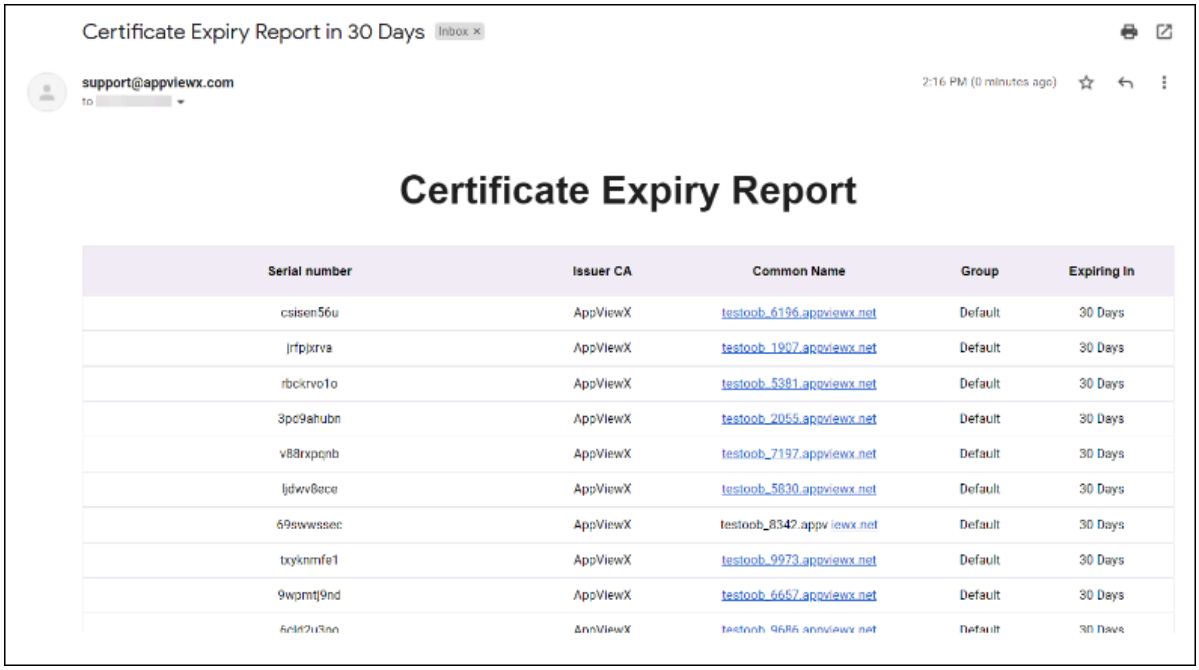


The following table describes the fields under the **Notifications** section:

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

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

- Email notification received with report as email content.

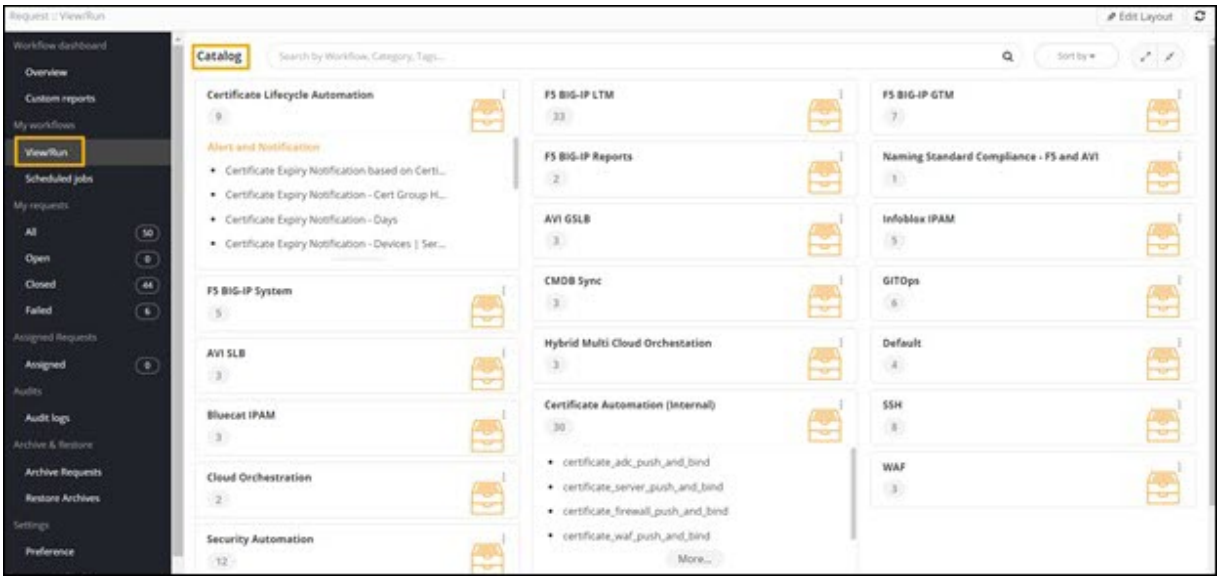


Update Certificate Attributes

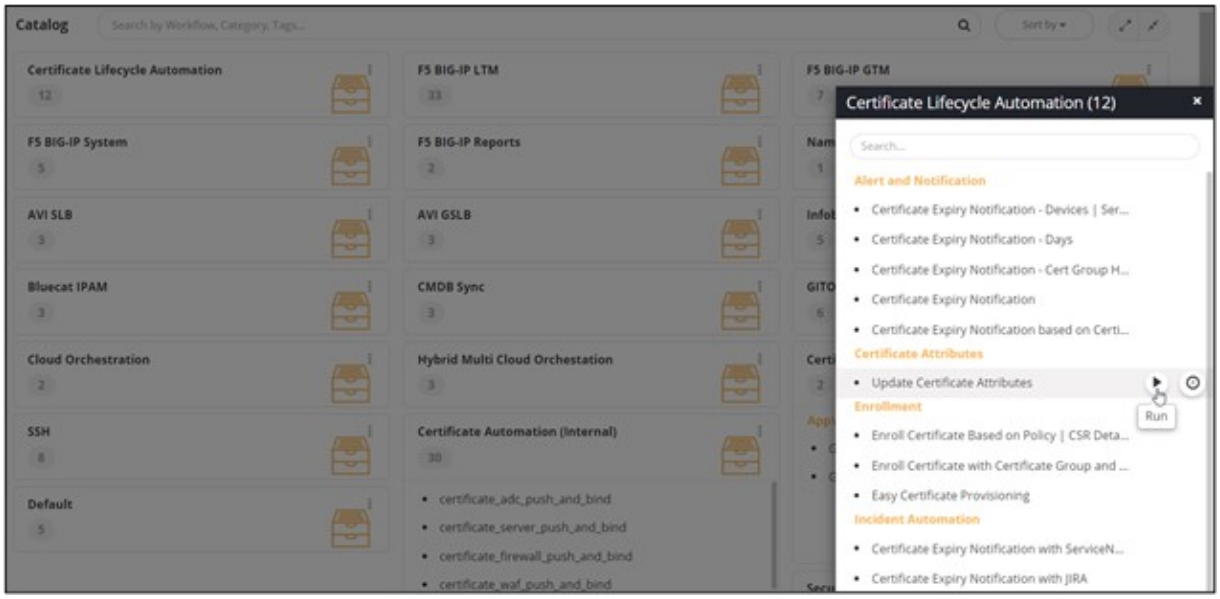
This workflow allows you to update the certificate attributes in bulk.

To trigger this workflow:

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

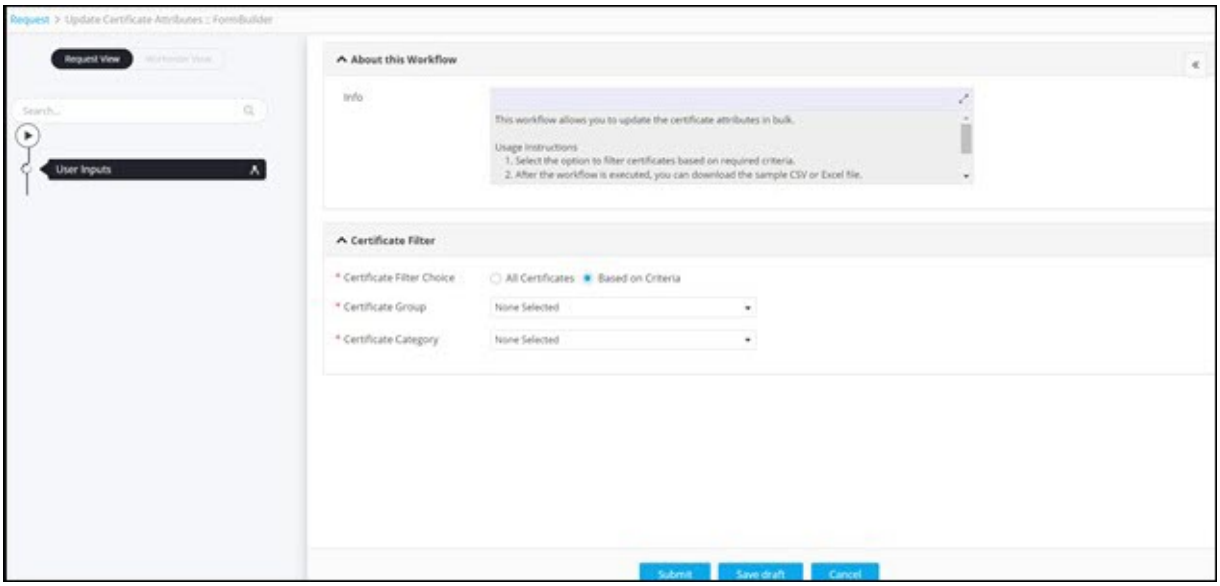


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Alert and Notification** category, hover your mouse over the **Update Certificate Attributes**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



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

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



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

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

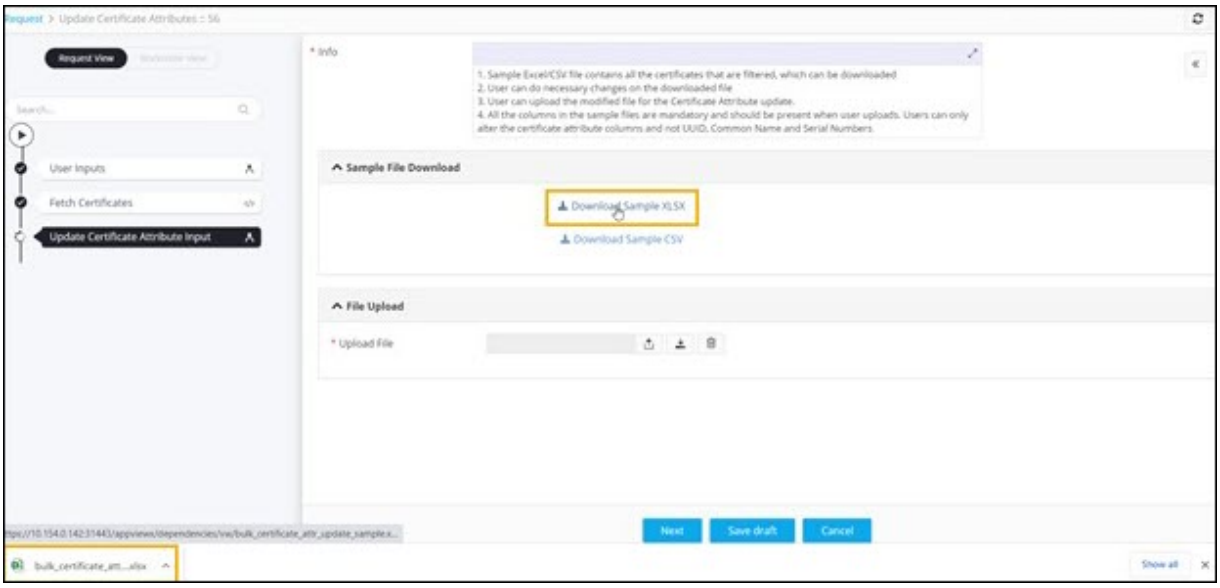
Field	Description
All asterisk (*) marked fields are mandatory.	

5. Click **Submit**.

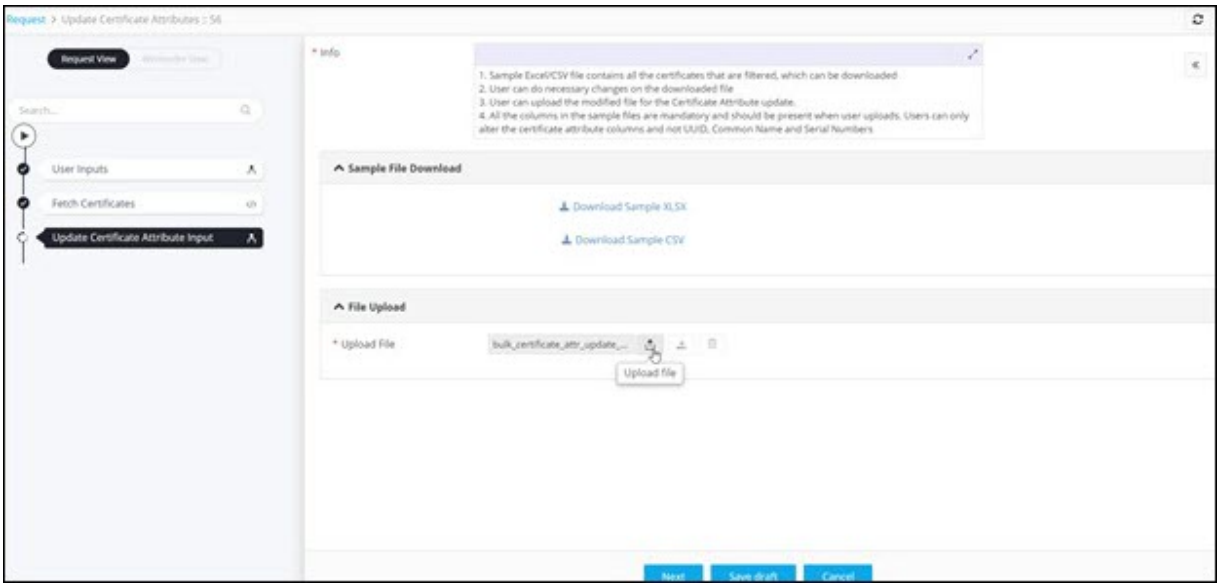
   Fetch Certificates task is executed.

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

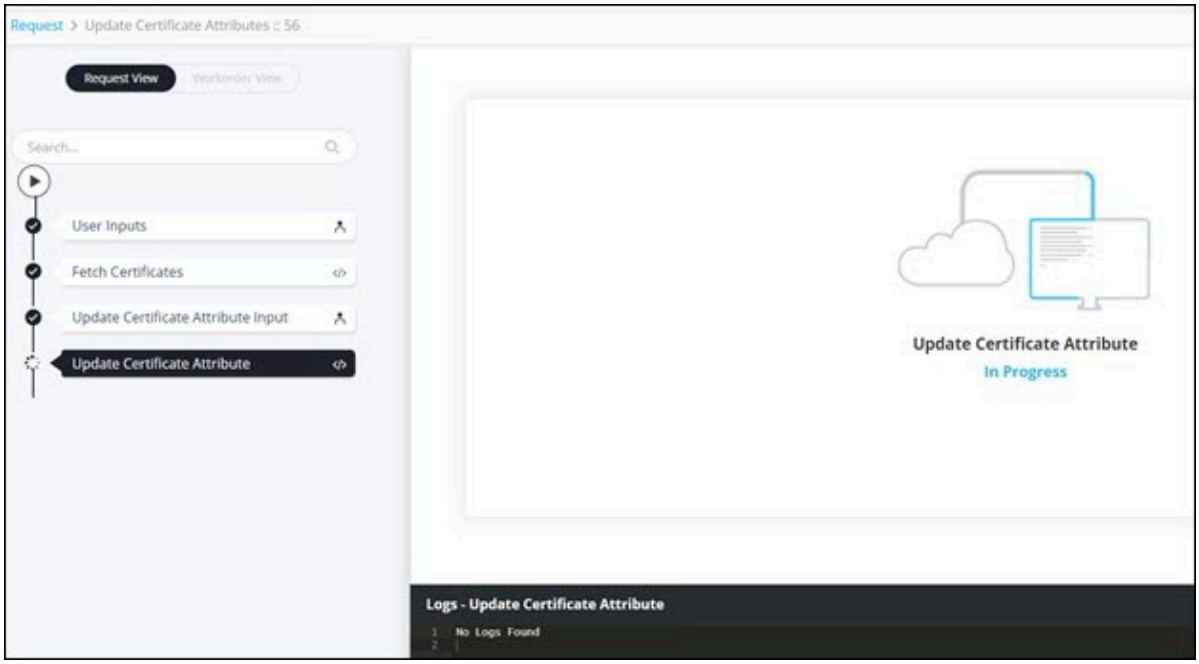
   The file is downloaded to your device.



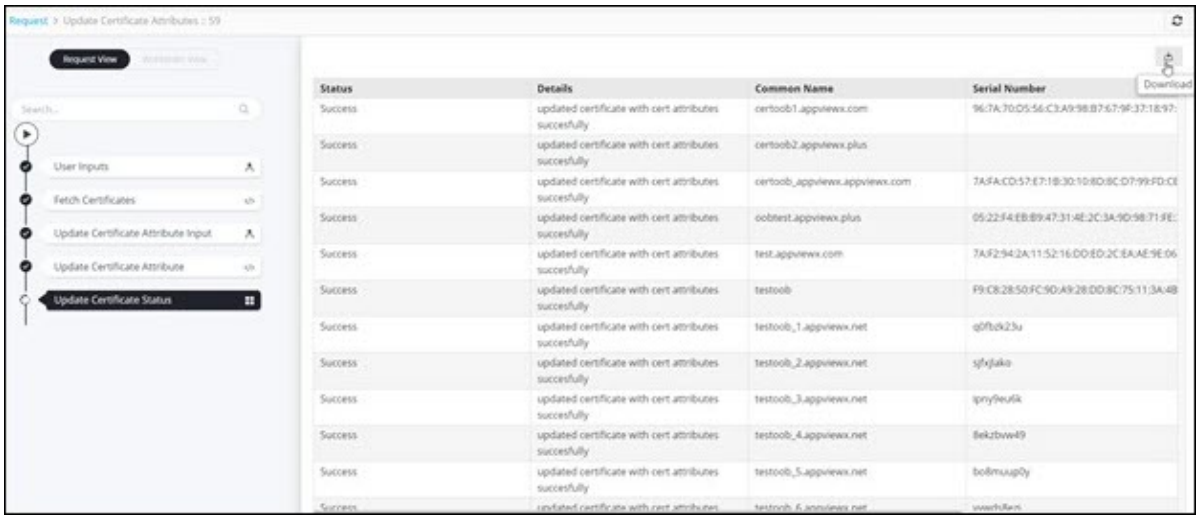
7. Once you have updated the certificate attributes in the downloaded file, under **File Upload**, click  to upload the modified file.



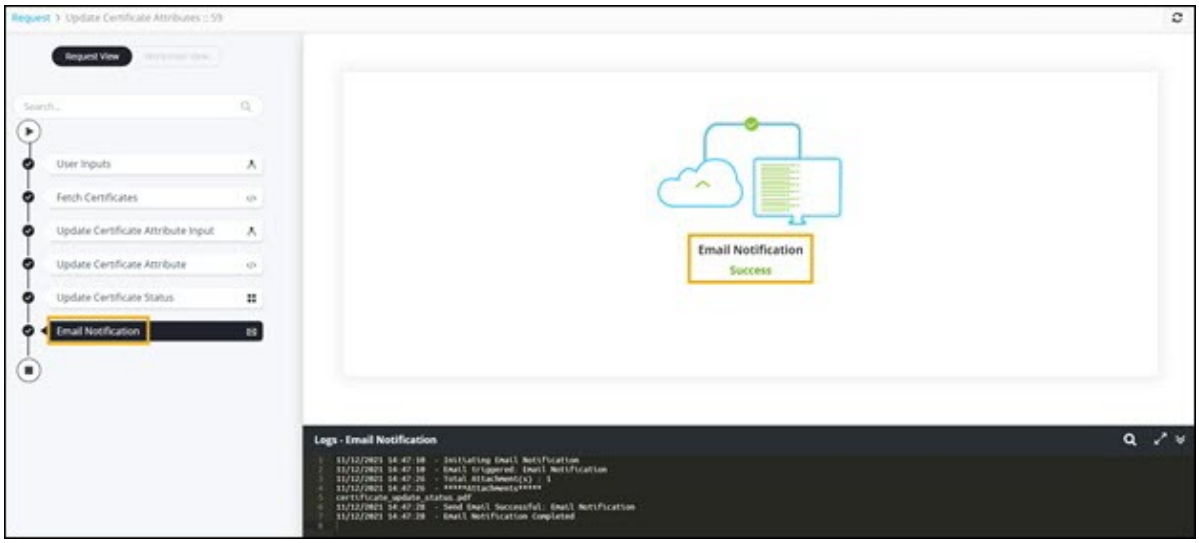
8. Click **Next**
9. In the **Confirmation** pop-up window, click **Ok**.
   - Update Certificate Attributes task in progress.



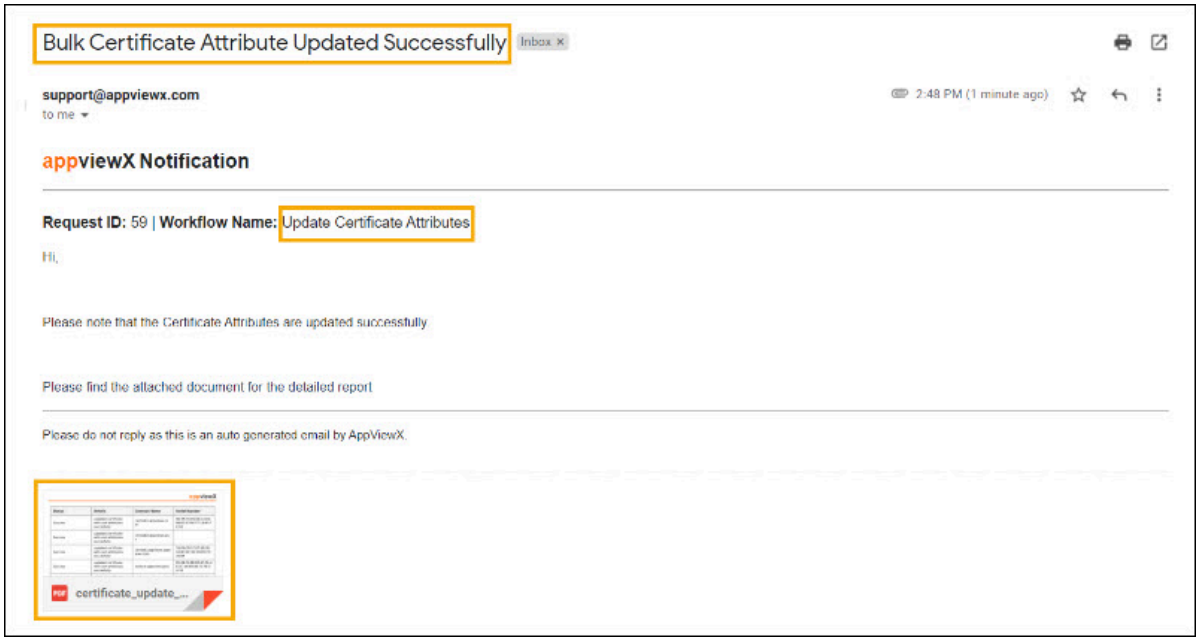
   - **Update Certificate Status** is displayed. To download this list, from the top right corner of the screen, click  .



• Email notification sent successfully.



- Email with report received.

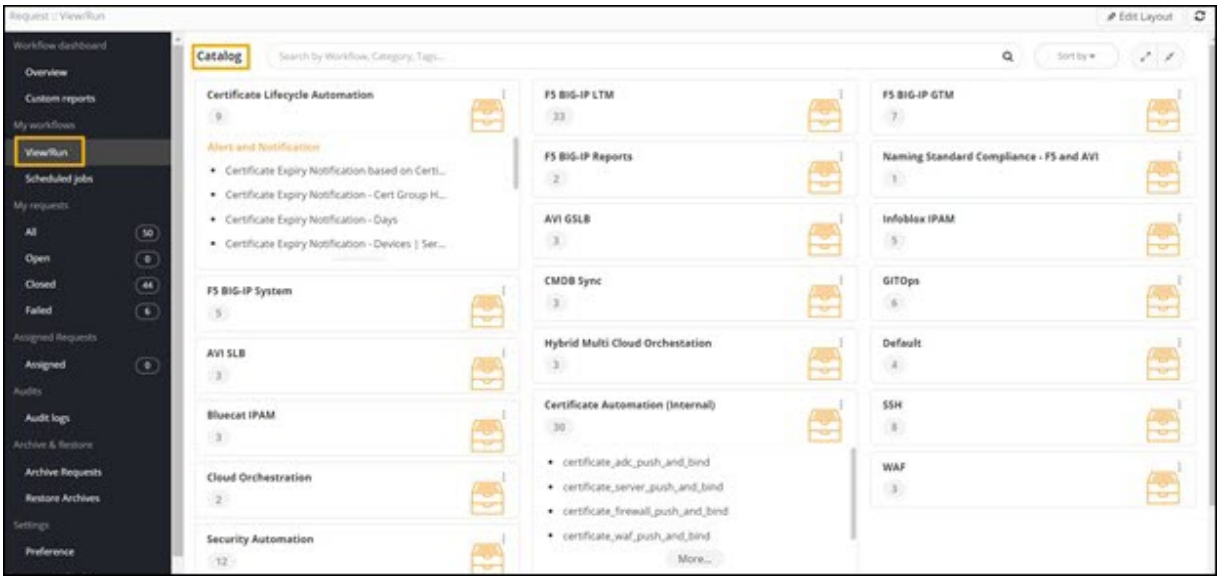


Certificate Expiry Notification with JIRA

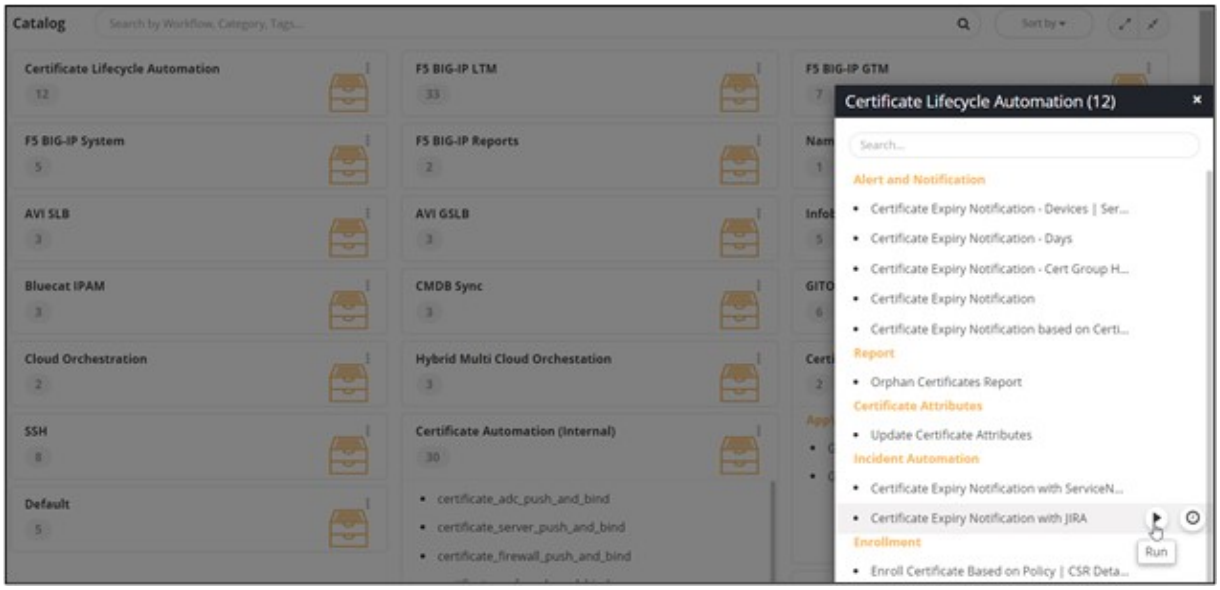
This workflow allows you to create a JIRA incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

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

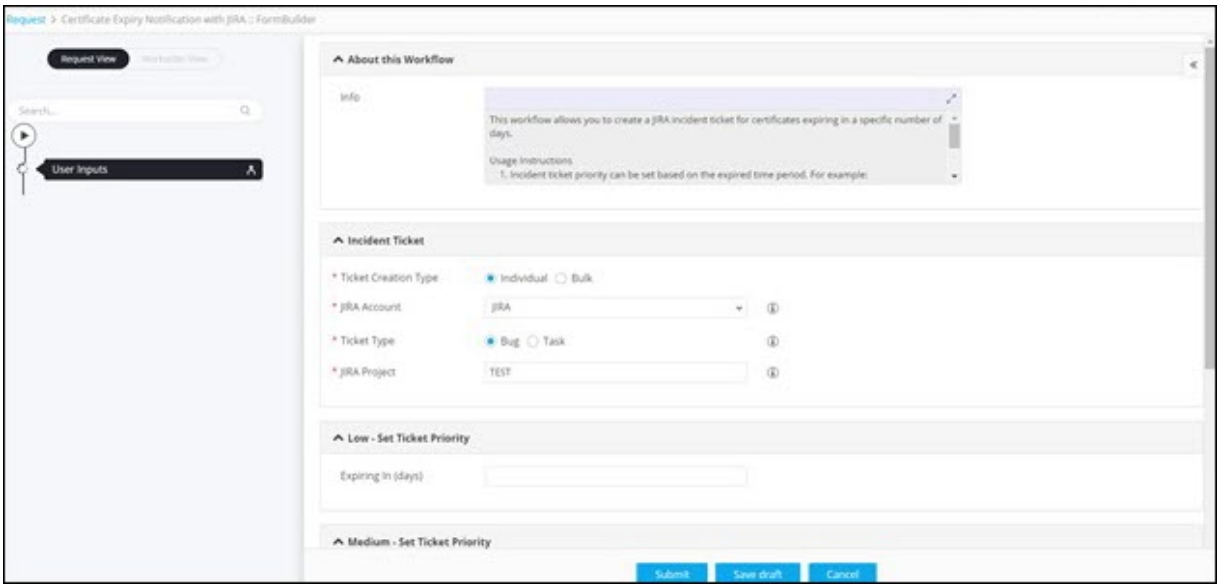


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

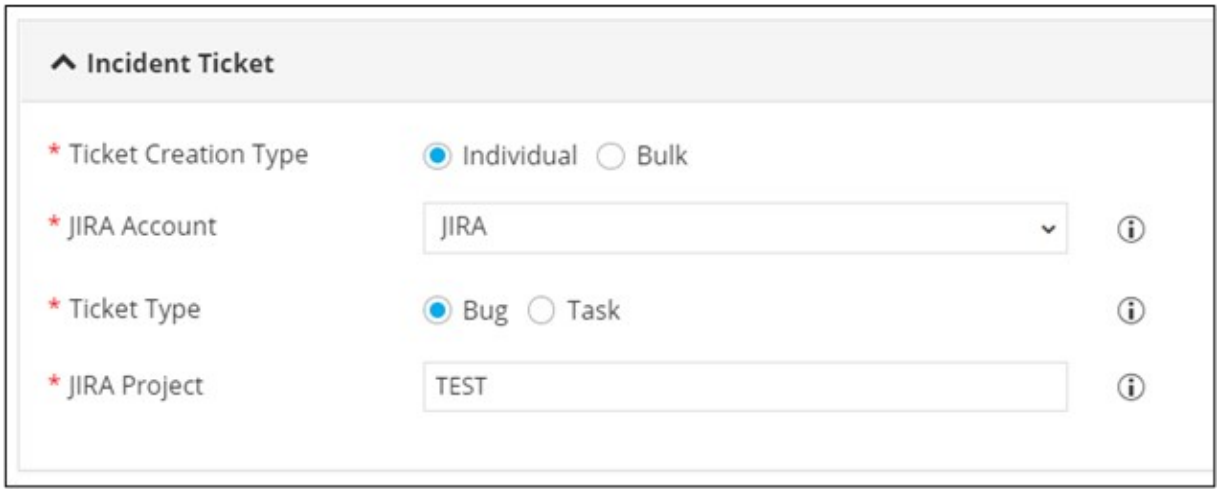


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



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



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

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

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: • **Bug -** This will indicate that the ticket is for a bug in the project. • **Task -** This will indicate that the ticket is for a task in the project. **Note: Bug** is the default selection.
***JIRA Project**	Enter the name of the project for which ticket(s) have to be raised. **Note: Test** is the default selection.
All Asterisk (*) marked fields are mandatory.	

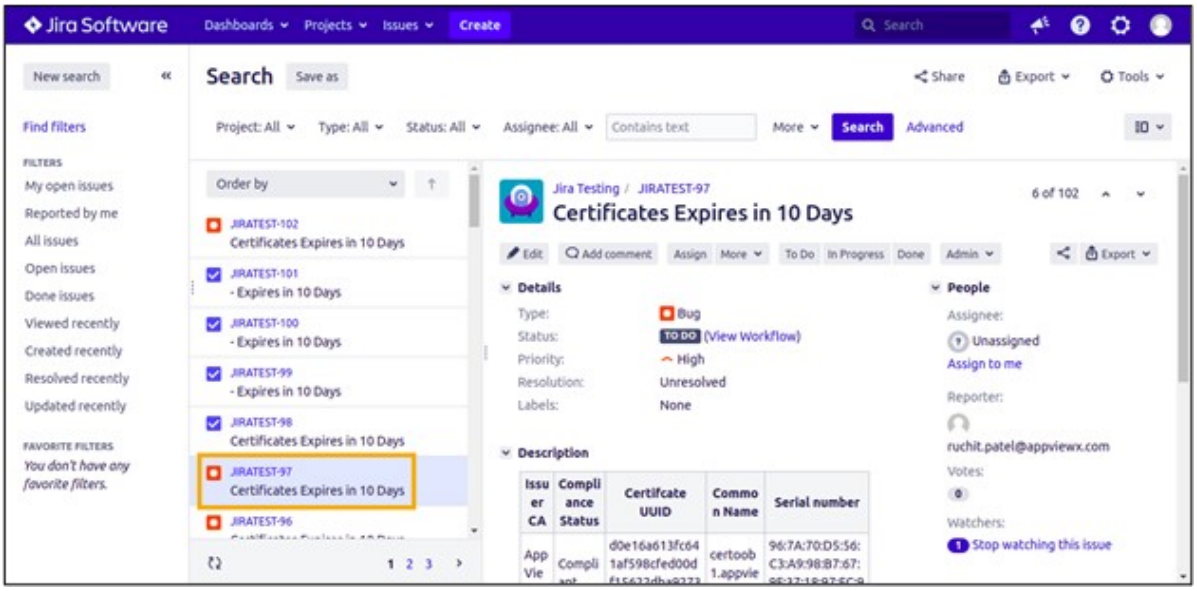
6. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
7. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for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

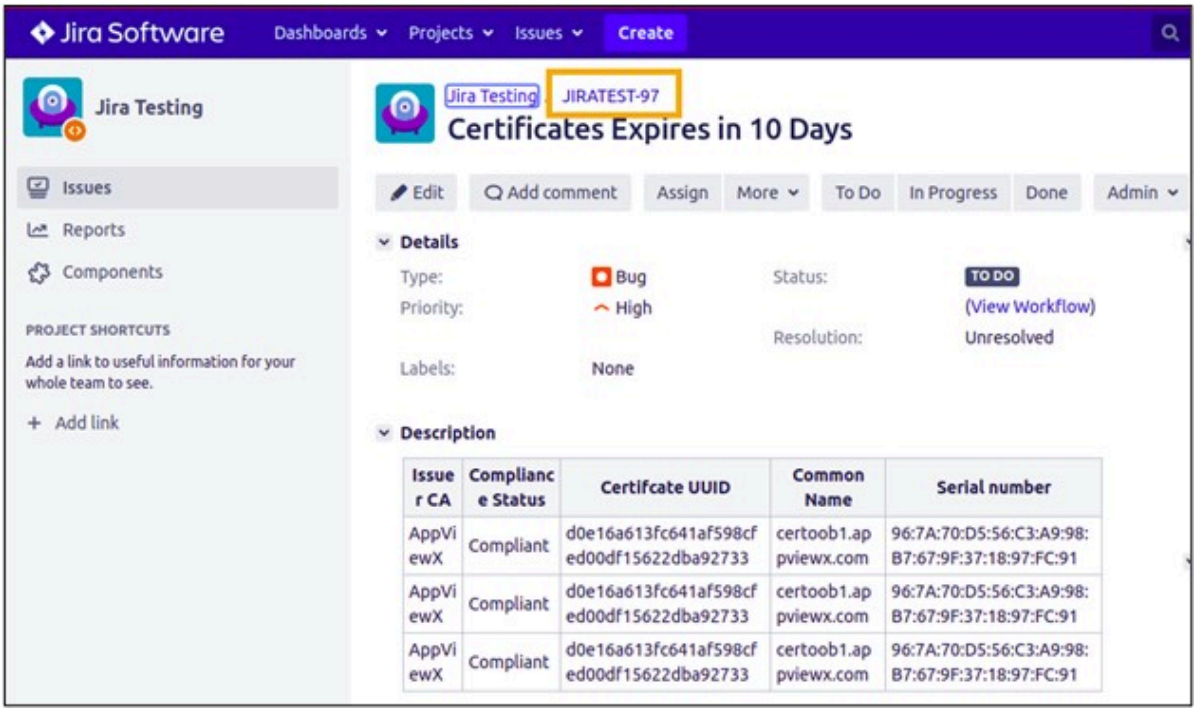
   Note: This is a mandatory field. Multiple certificate attributes can be displayed by selecting the checkbox of the attribute name.

10. Click **Submit**.

- JIRA ticket creation Summary.

- Ticket created on Jira.



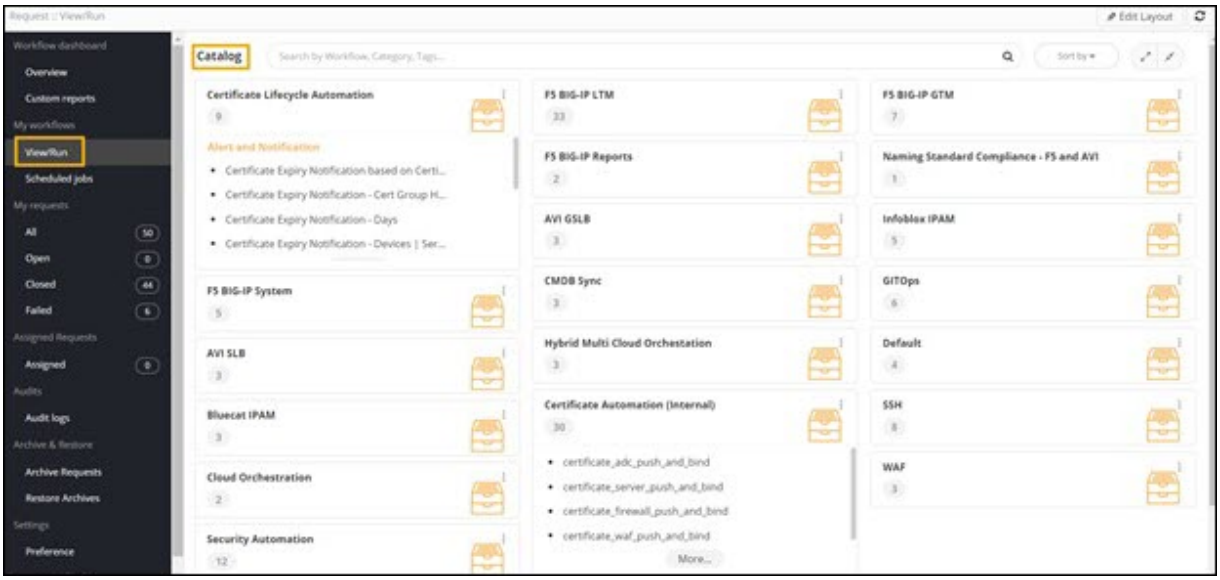


Certificate Expiry Notification with ServiceNow

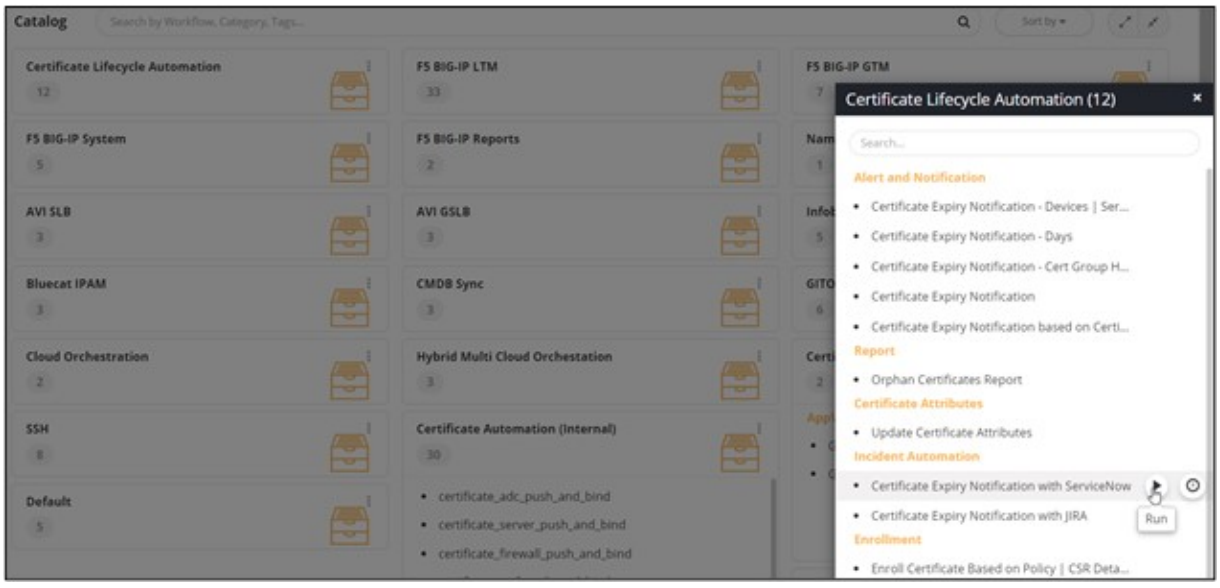
This workflow allows you to create a ServiceNow incident ticket for certificates expiring in a specific number of days.

To trigger this workflow:

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

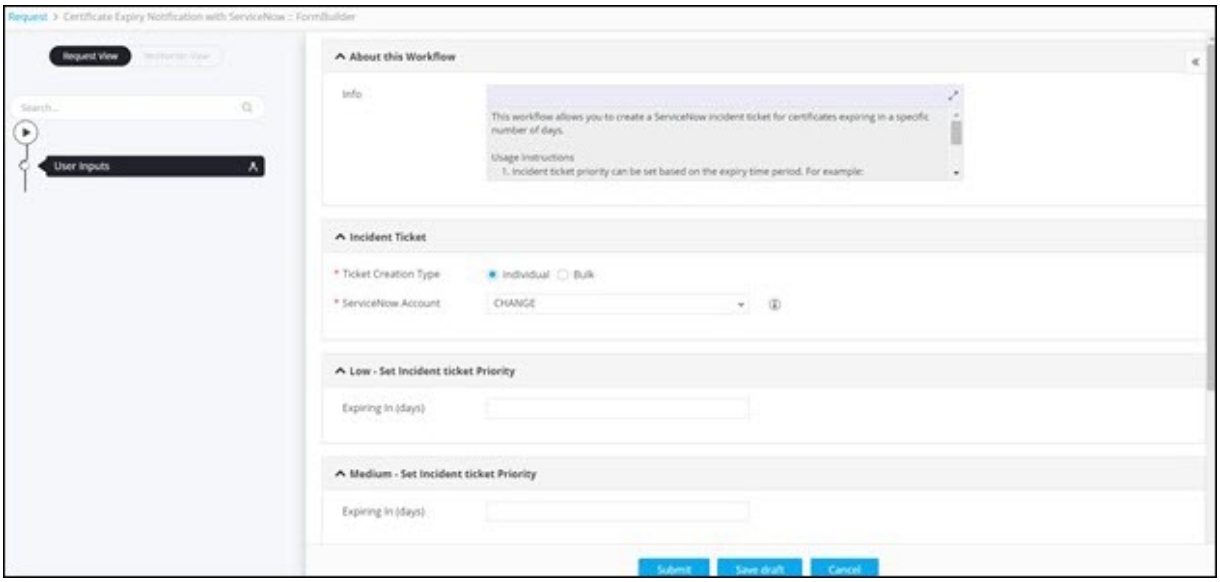


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Incident Automation** category, hover your mouse over the **Certificate Expiry Notification with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

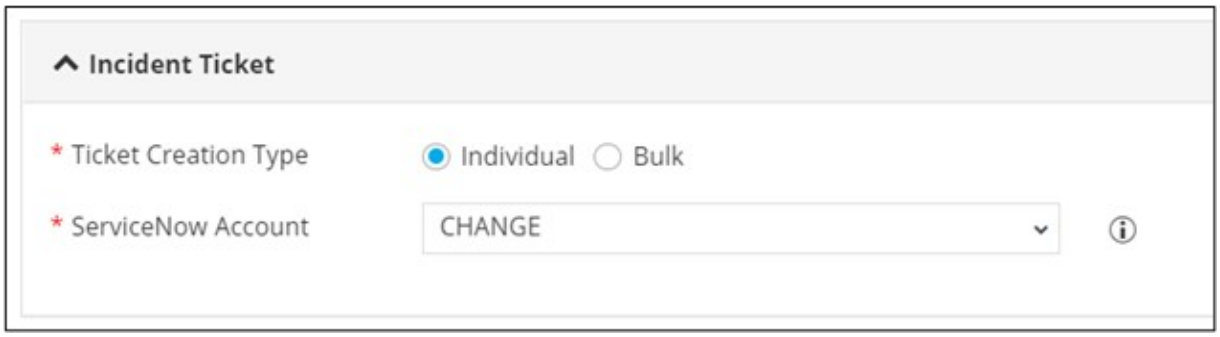


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



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



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

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

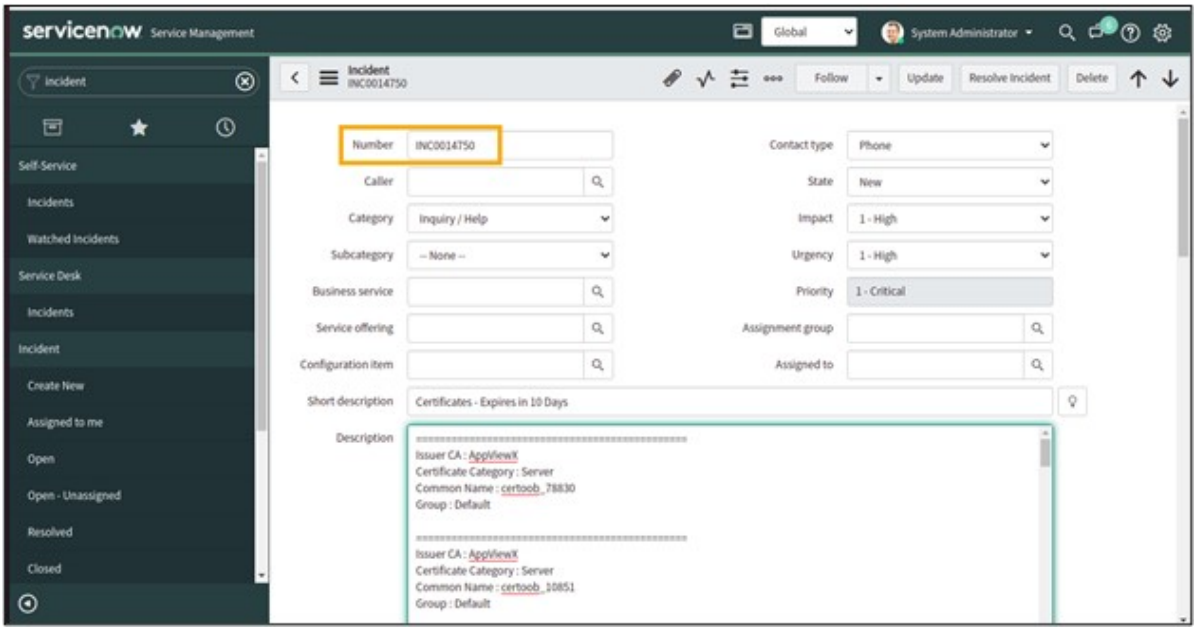
Field	Description
	Note: Change is the default selection.
All Asterisk (*) marked fields are mandatory.	

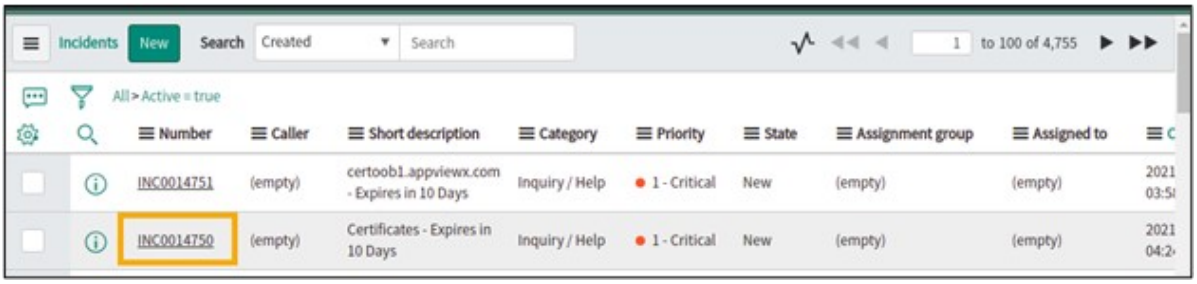
6. Under the **Low - Set Incident ticket Priority** section, enter a value (number of days) for tickets with low priority. For example, for certificates expiring in 90 days, incident priority can be low.
7. Under the **Medium - Set Incident ticket Priority** section, enter a value (number of days) for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

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

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

    - Incident ticket created on ServiceNow.



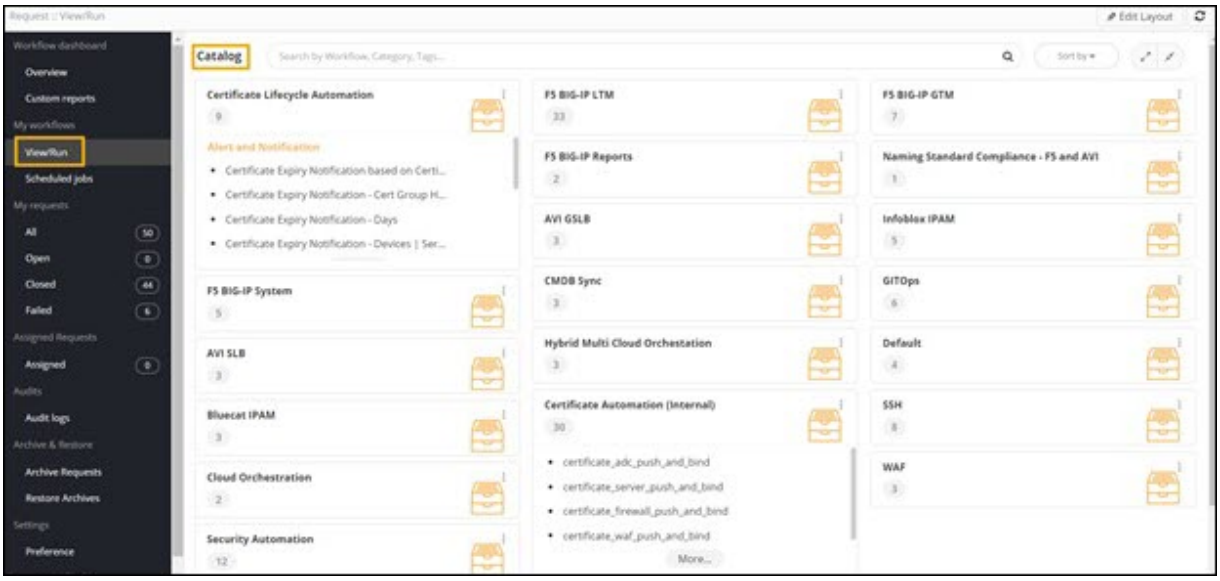


Orphan Certificates Report

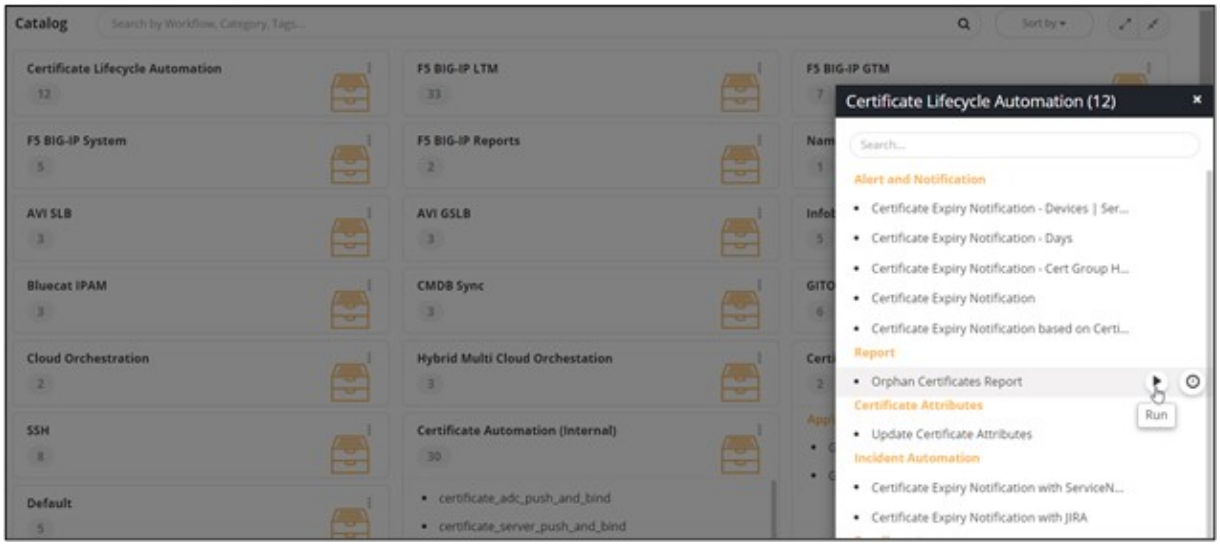
This workflow enables you to generate a report on certificates that are present on a device but not associated with any application or profile.

To trigger this workflow:

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

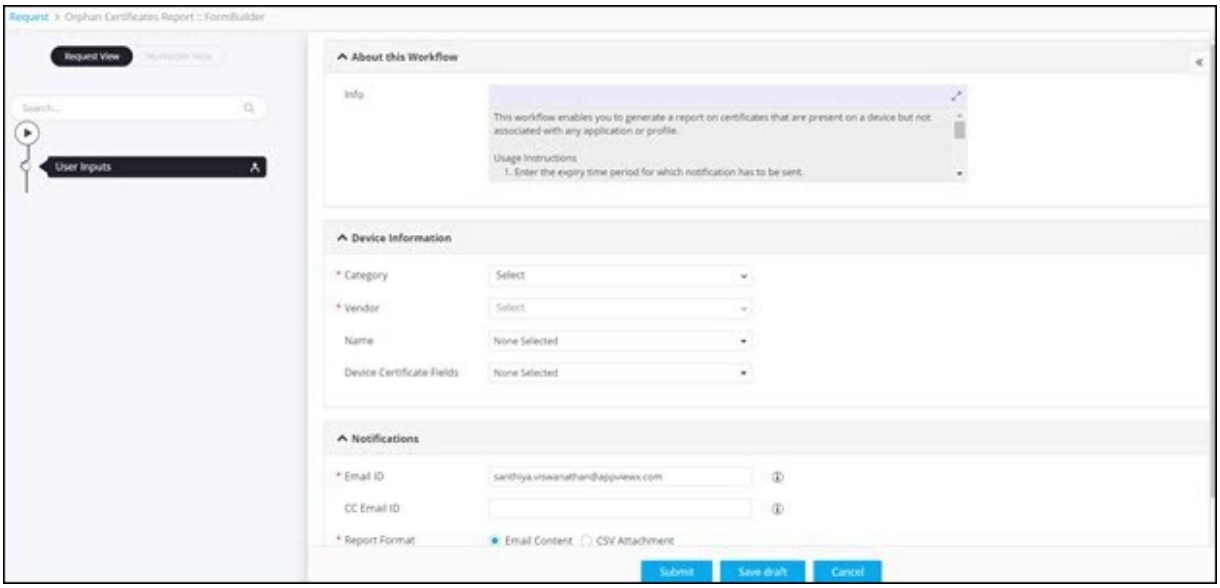


2. On the **Catalog** page, under **Certificate Lifecycle Automation** catalog, click .
3. From the options displayed, select **Full View**.
4. In the **Certificate Lifecycle Automation** window, under the **Report** category, hover your mouse over the **Orphan Certificates Report** workflow and click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

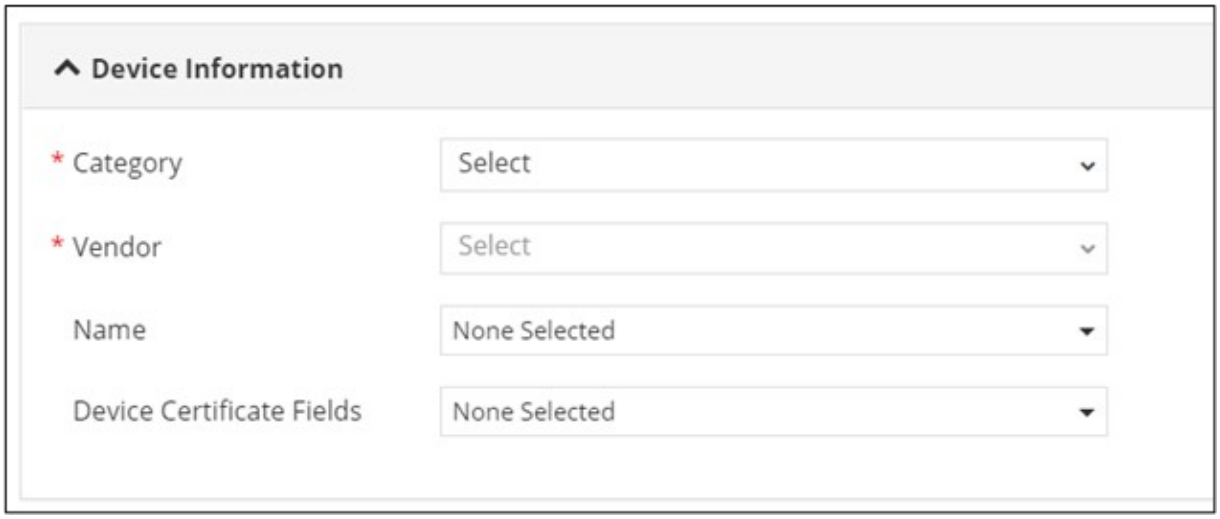


Tip: You can also search for the workflow by typing the workflow name in the search bar.

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



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

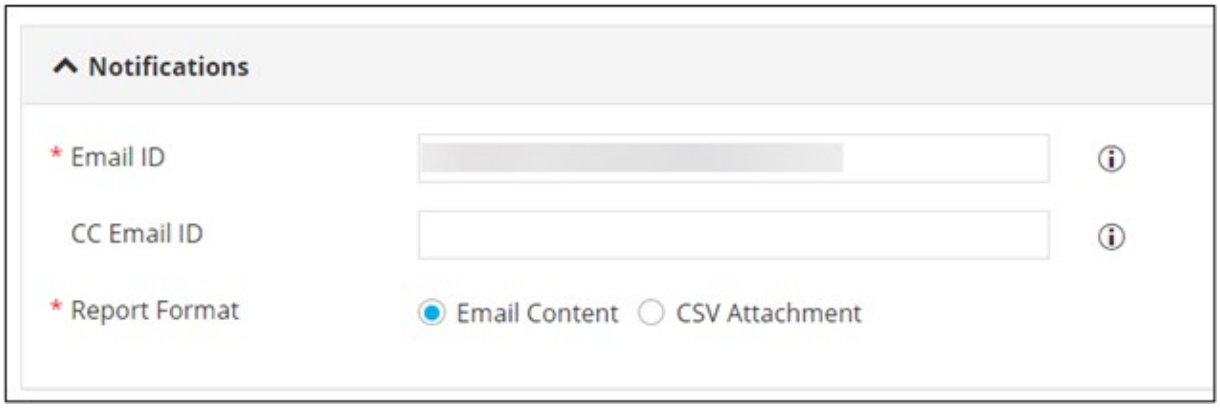


The following table describes the fields in the **Device Information** section:

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

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

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

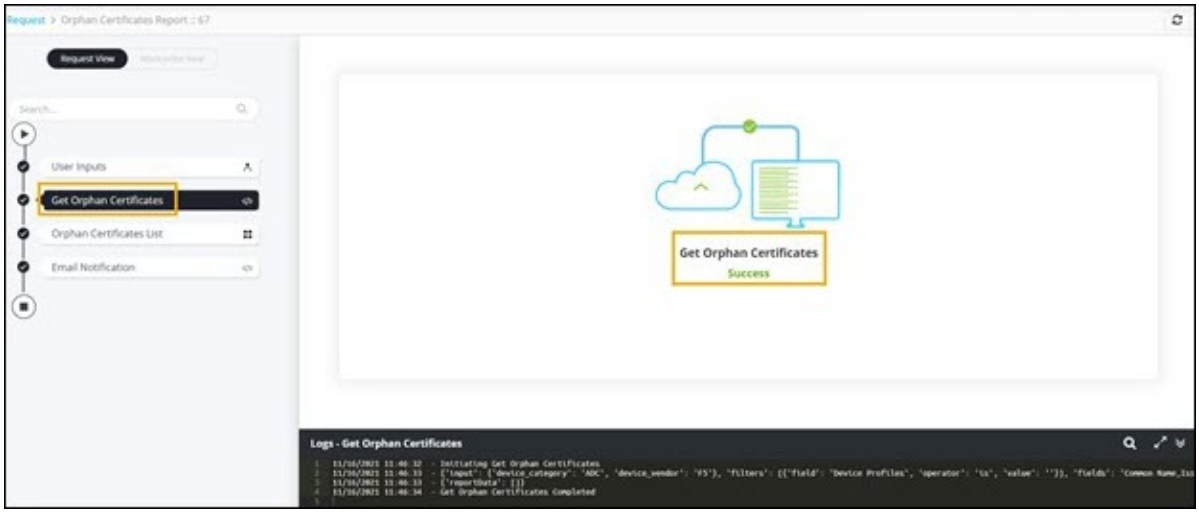


The following table describes the fields in the **Notifications** section:

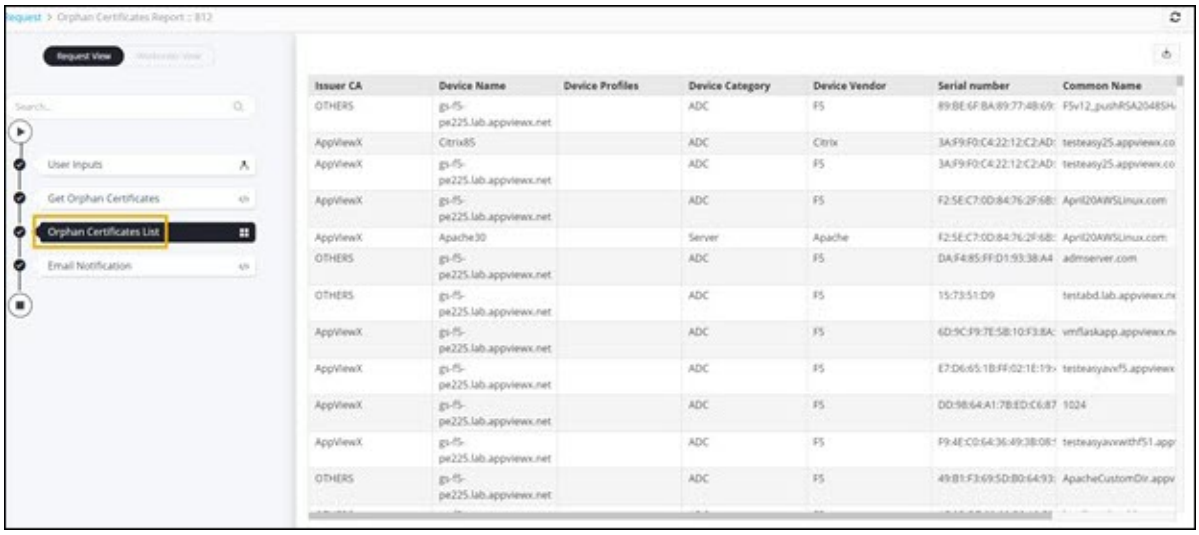
Field	Description
***Email ID**	Enter the email address of the recipient in the 'To' field. Comma separated values can be entered for multiple email addresses. **Note:** The email id of the logged in user is populated automatically.
CC Email ID	Enter the email address of the recipient in the 'CC' field.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

7. Click **Submit**.

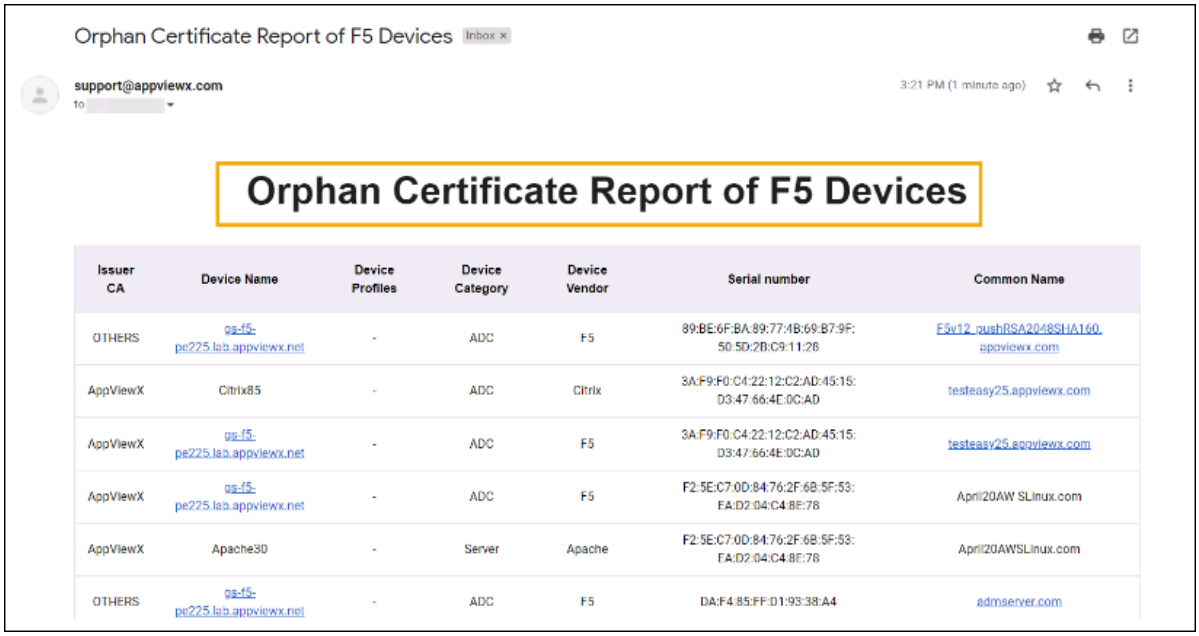
• Get Orphan Certificates task executed.



• Orphan Certificates List generated.



- Email notification received with report as email content.



Orphan Certificate Report of F5 Devices Inbox ×

support@appviewx.com
to

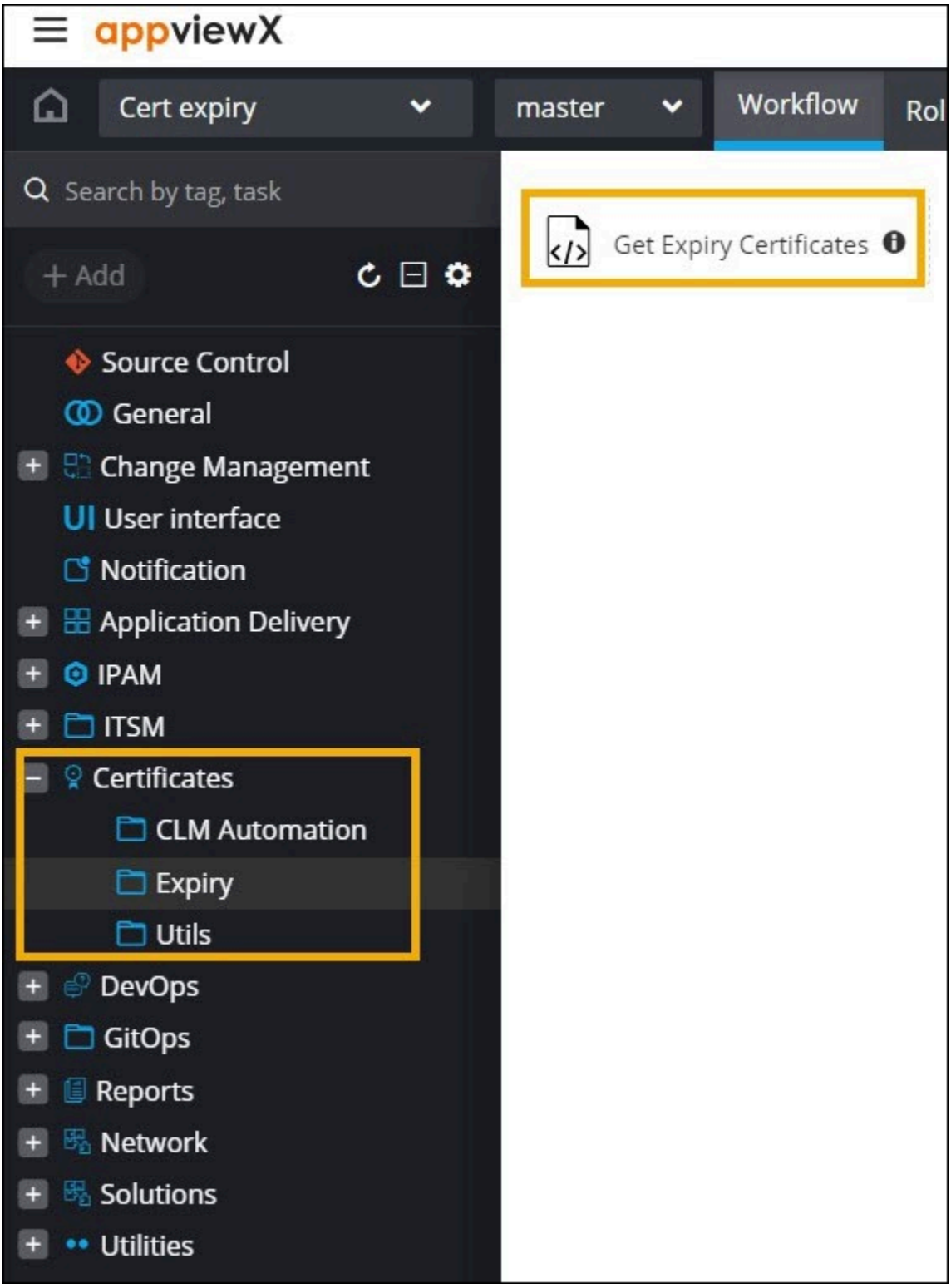
3:21 PM (1 minute ago)

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:89:77:4B:69:B7:9F:50:5D:2B:C9:11:28	F5v12_pushRSA2048SHA160.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:6B:5F:53:EA:D2:04:C4:8E:78	April20AW SLinux.com
AppViewX	Apache30	-	Server	Apache	F2:5E:C7:0D:84:76:2F:6B:5F:53:EA: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

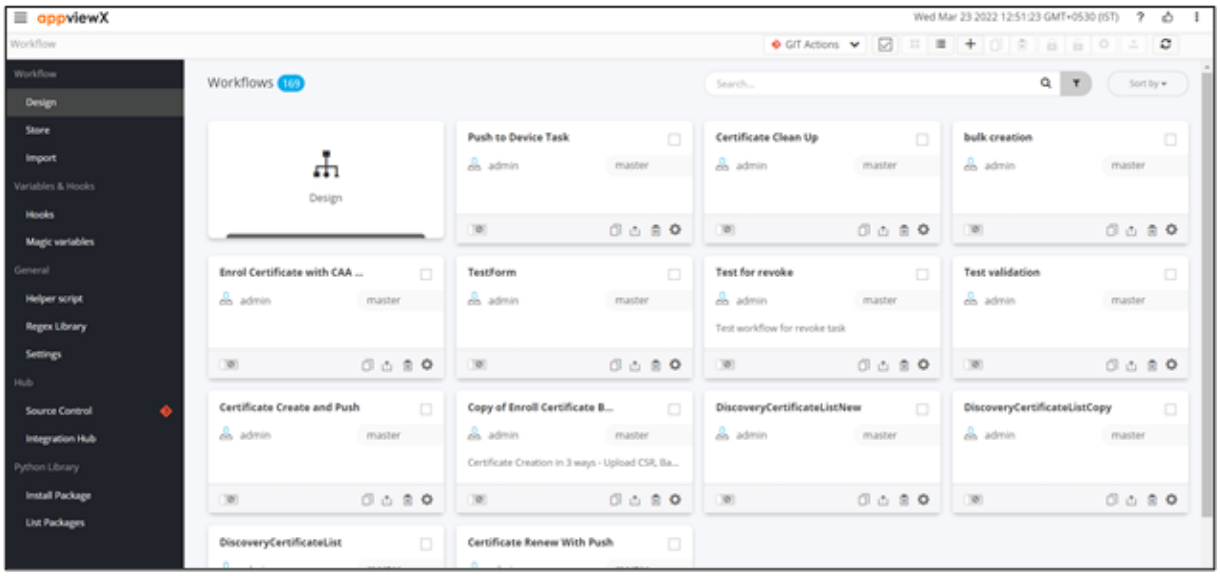
You can design a custom workflow for receiving certificate expiry notifications using the prebuilt task for getting expiry certificates available in the Workflow Studio. The OOB script task for getting expiry certificates can be found under **Certificates**, in the **Expiry** folder in the Workflow Studio.



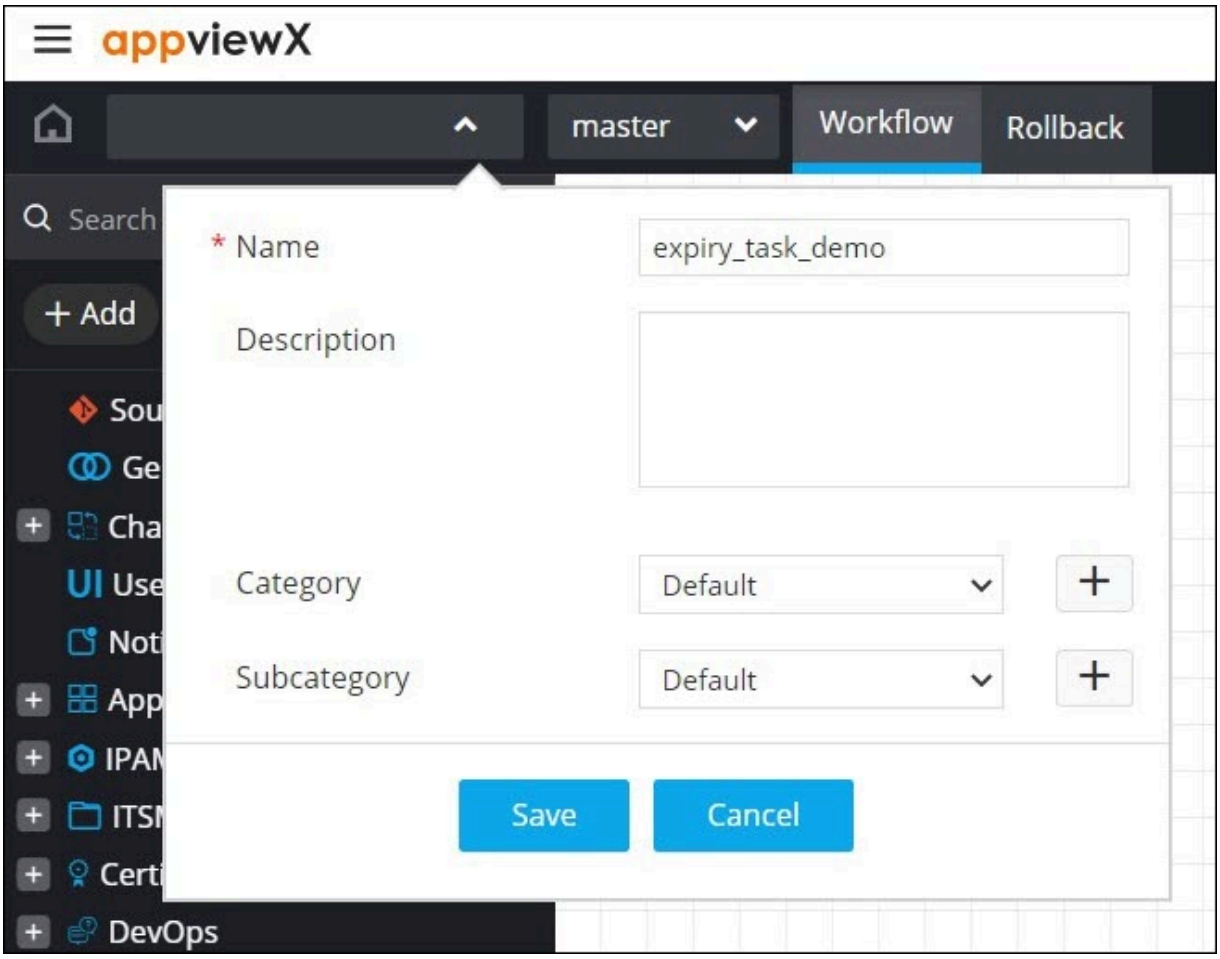
To design a custom workflow using the **Get expiry certificates** task

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

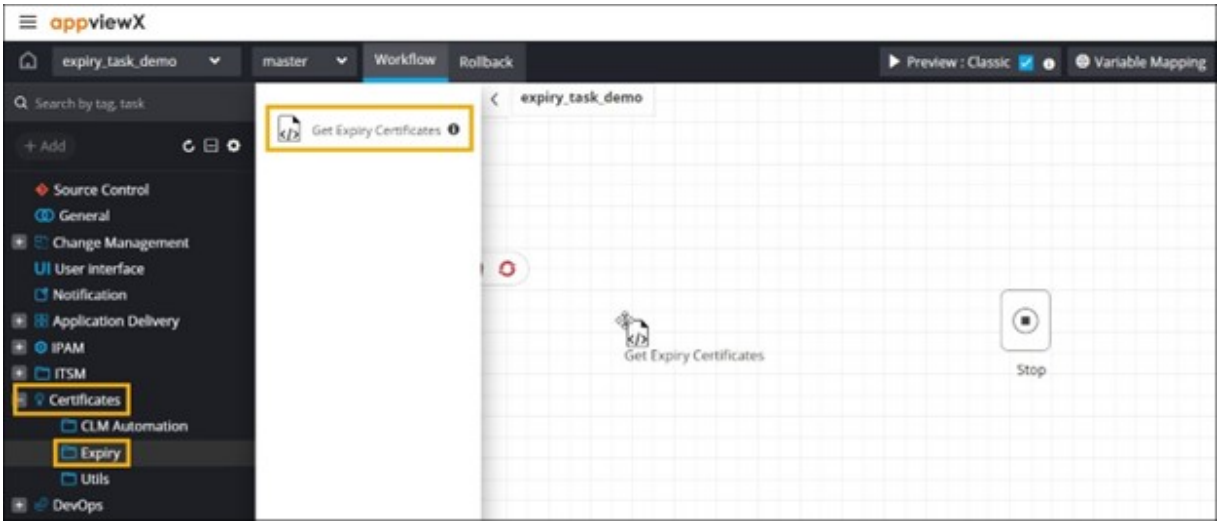
   The **Workflow** inventory page is displayed.



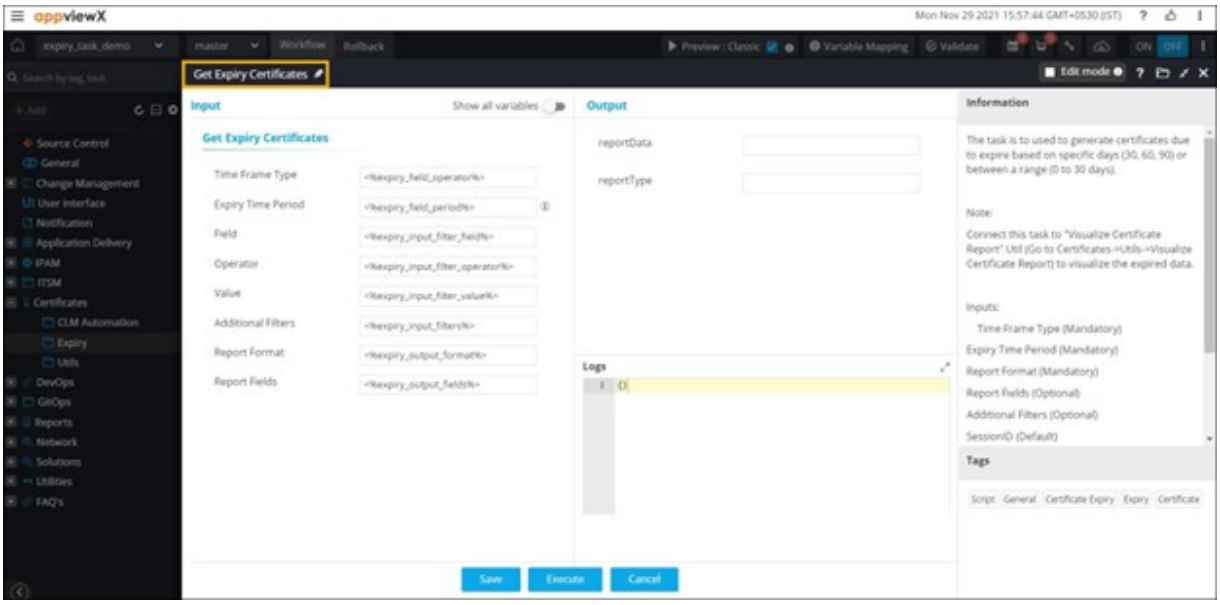
3. On the **Workflow** inventory page, click **Design**.
4. Enter a suitable **Name** for the workflow.
5. Click **Save**.



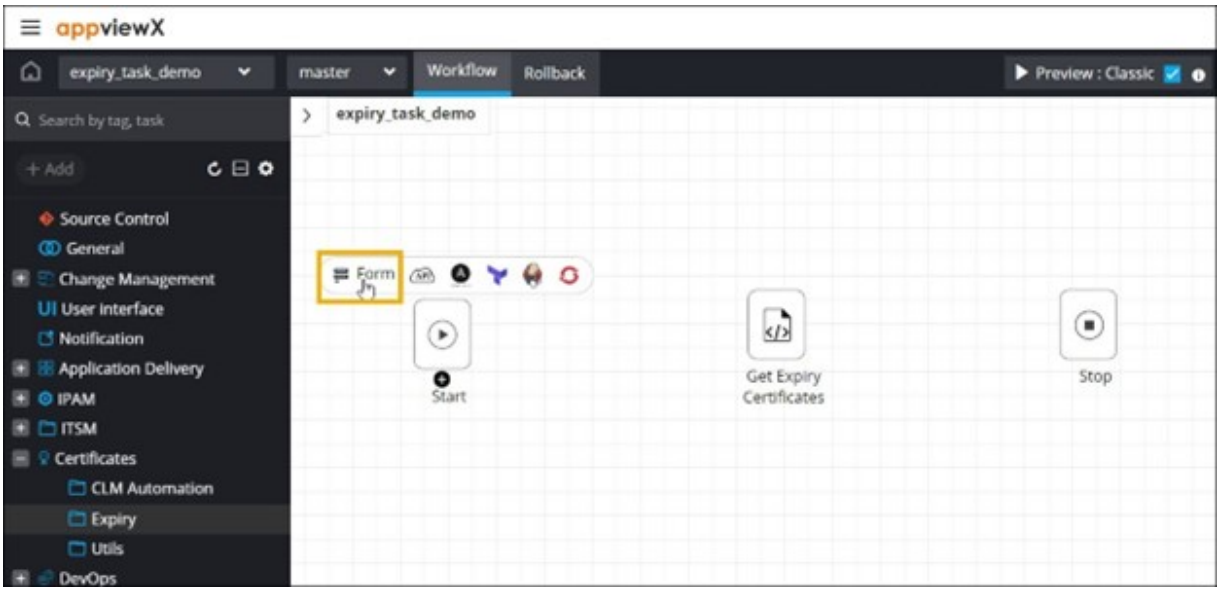
6. From the **Certificates** folder, under **Expiry**, drag and drop the **Get Expiry Certificates** task.



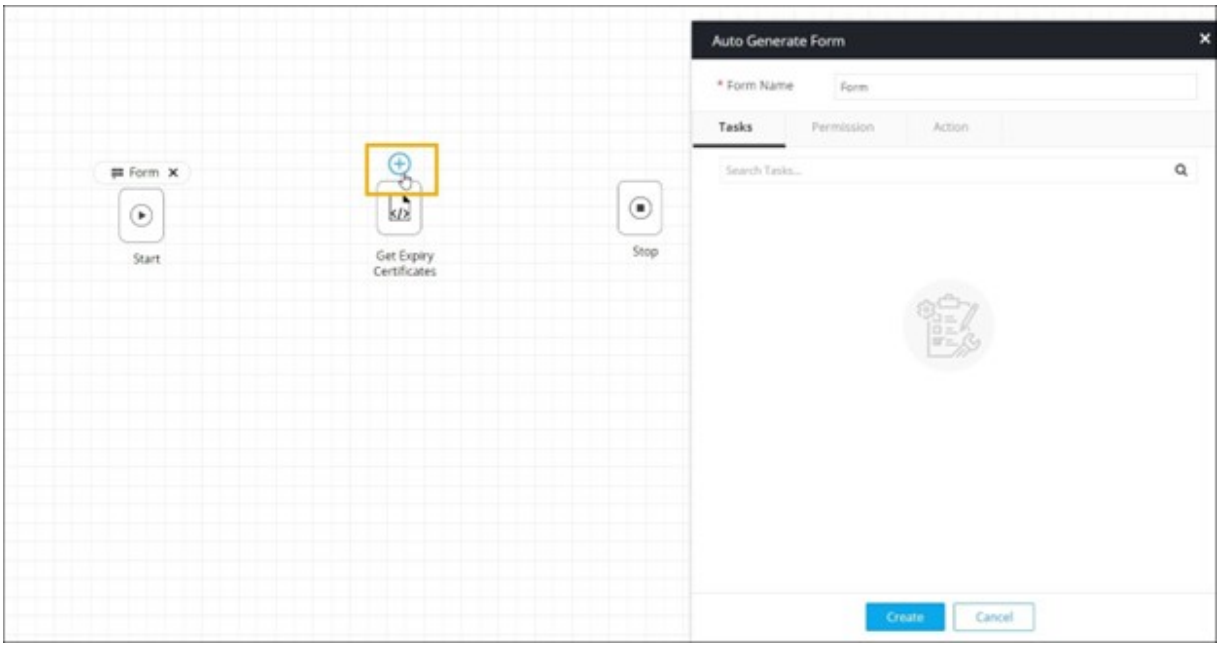
This task can be used to generate a report listing certificates due to expire in a specific number of days.



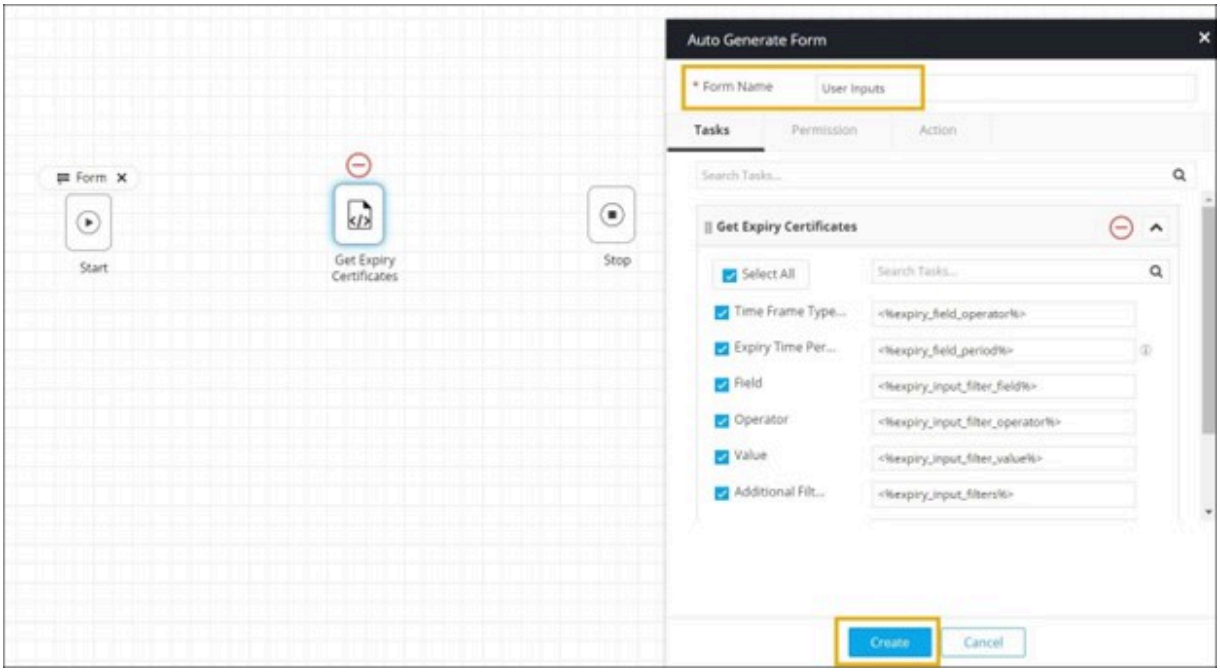
7. To auto-generate a form for this workflow, click **Form** above the **Start** task.



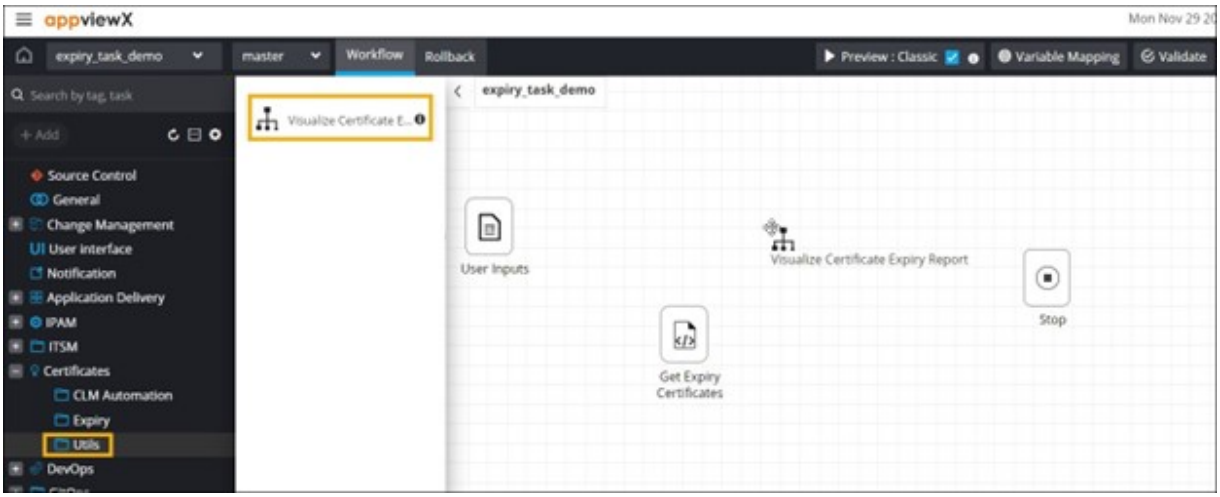
8. Click ⊕ above the **Get Expiry Certificates** task to auto-populate the form fields.



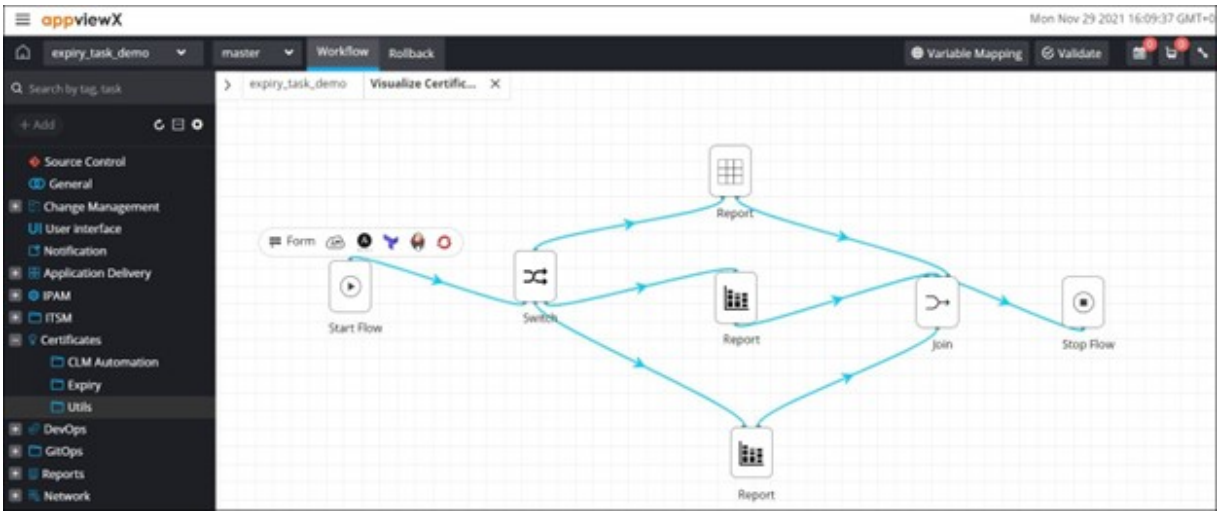
9. Select the fields required in the input form.
10. Provide a **Form Name** and click **Create**.



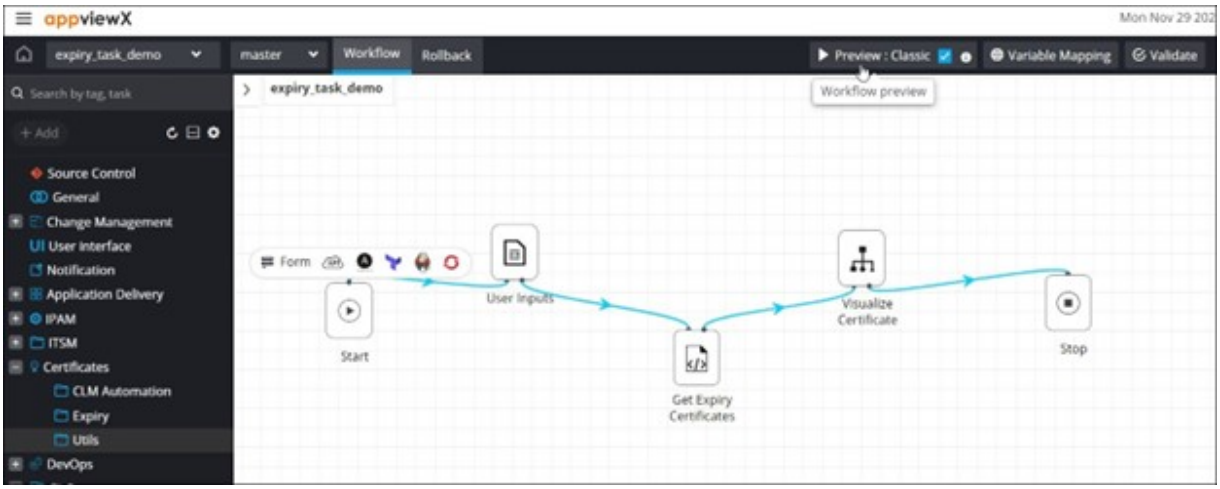
11. To display the certificate data in a report, from the **Utils** folder, drag and drop the **Visualize Certificate Expiry Report** prebuilt subflow.



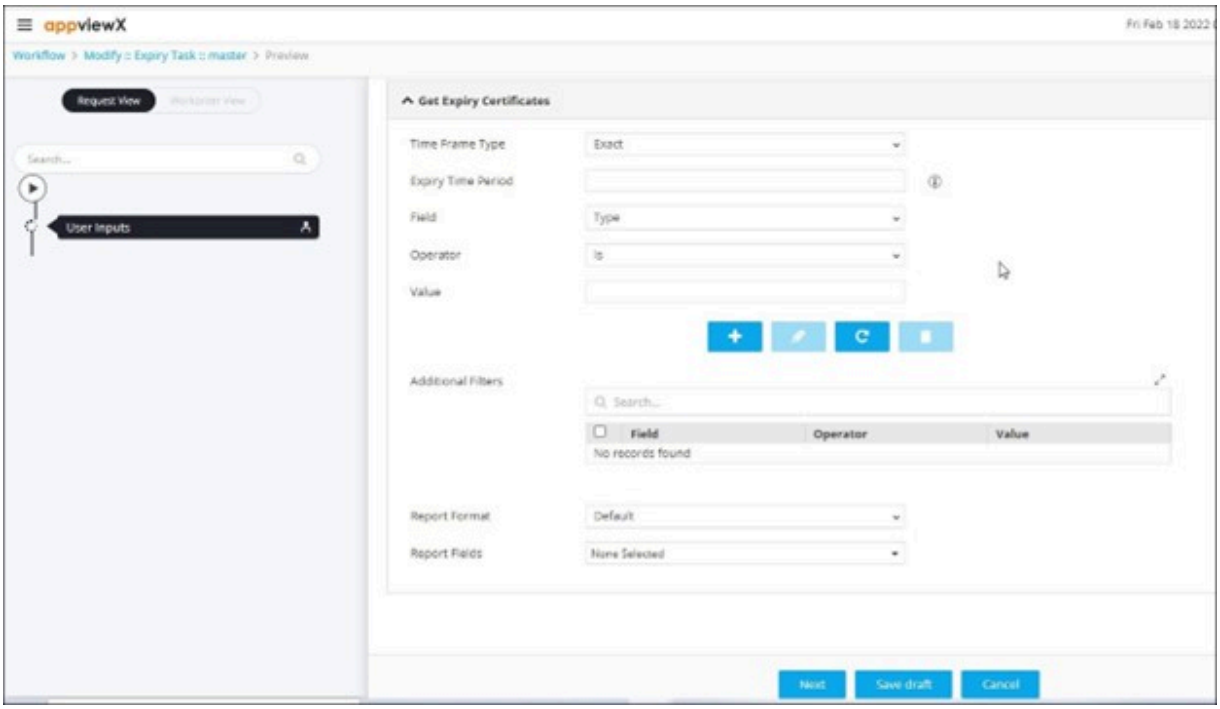
This subflow includes User Interface tasks such as Grid and Chart (Pie chart and Stacked bar chart). The report generated will be displayed as a grid or a chart based on the inputs provided in the input form.



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



User Inputs form is displayed.



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

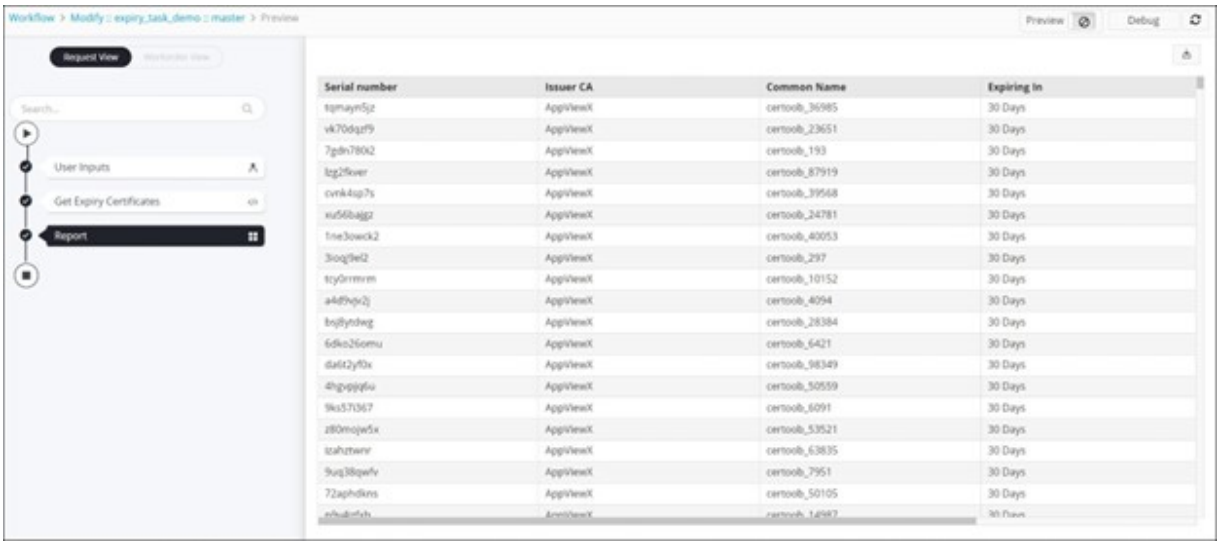
Field	Description
Time Frame Type	Enter the time frame type from the available options: • **Exact -** Allows you to enter the exact value for the expiry time period (30 days). • **Range -** Allows you to give a range for the expiry time period (0 - 30).

Field	Description
	Note: Exact is the default selection.
Expiry Time Period	Enter the expiry time period for which notification has to be sent. Multiple values can be entered, separated by commas. You can either define it as an exact number or a range or a combination of both. For example, 30,60,90 or 0-30,30-60,0-60 or 30,30-60,90. • **Input type: Range** - The expiry report will be generated for the range specified. For example, 0 - 30 days, 0 - 60 days, 0 - 90 days. • **Input type: Exact** - The expiry report will be generated for certificates expiring on the exact specified date. For example, certificates expiring on the 30th, 60th, 90th day.
Field	Select the field from the options available in the dropdown.
Operator	Select the conditional operator: • **Is** • **Is Not**
Value	Enter a valid value for filtering the certificates.
Additional Filters	This grid displays the values selected in these fields: • **Field** • **Operator** • **Value** **Note:** The steps to apply these additional filters are given below the table.
Report Format	Select the format in which the report is displayed from the available options: • **Default** • **Pie Bar Chart** • **Stacked/Bar Chart**
Report Fields	Select the fields to be displayed in the report from the options available in the dropdown.

13. To add filters to the **Additional Filters** grid, click .
14. To edit the value of a particular filter, select the filter in the grid and click .
15. 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.



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.