

# Delete Expired Certificates from F5 Workflow Guide



**Copyright © 2017 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.

This product includes software developed by the CentOS Project ([www.centos.org](http://www.centos.org)).

This product includes software developed by Red Hat, Inc. ([www.redhat.com](http://www.redhat.com)).

This product includes software developed by the VMware ([www.vmware.com](http://www.vmware.com)).

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

**Contact Information**

AppViewX, Inc.

500 Yale Avenue North, Suite 100

Seattle, WA 98109

Tel: +1 (206) 207 7541

Email: [info@appviewx.com](mailto:info@appviewx.com)

Web: [www.appviewx.com](http://www.appviewx.com)

**Document Information**

Software Version: 12.2.0

Document Version: 1.0

Last updated on: December 18, 2017

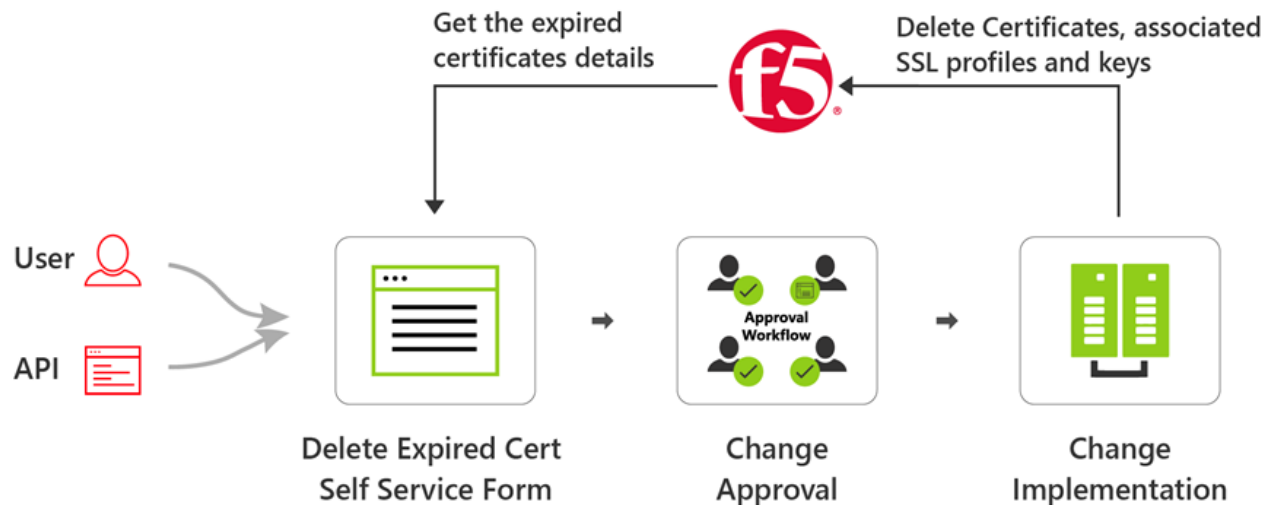
## Contents

Description .....	1
Prerequisites.....	1
Compatible Software Versions.....	1
Limitations .....	1
Log In to AppViewX.....	2
Add an ADC Device: F5 LTM.....	2
Import Visual Workflows.....	3
Import Helper Scripts .....	4
Enable a Workflow .....	5
Delete Expired Certificates from F5 workflow .....	5
WorkOrder flow .....	6
Request Inventory .....	8
Schedule a Workflow .....	8
View Scheduled workflows .....	9
Add a Credential .....	9
Troubleshooting .....	10

## Description

The Delete Expired Certificates from F5 workflow is used to delete the expired certificates and its associated SSL profiles and keys from an F5 device. The configuration to delete the expired certificate and key from an F5 device are reviewed and approved at AppViewX. After the approval is granted, the workflow will delete the expired certificate from an F5 device. If an expired certificate is associated to any SSL profile, it is deleted from the F5 device only after the certificate and the key of that particular profile are replaced with the default certificate and key.

The Delete Expired Certificates from F5 flow diagram is shown in the image below:



## Prerequisites

To run this automation workflow in your environment, ensure that the following pre-requisites are met:

- Free AppViewX or AppViewX version 12.1.0 and 12.2.0 has been downloaded and installed.
- The ADC devices has been added in the AppViewX inventory with a Data center name.
- Each ADC device is a managed entity in AppViewX.
- You have administrator permissions to add a device to the AppViewX inventory.

## Compatible Software Versions

The workflow has been tested and validated on the following software versions:

- AppViewX – Free AppViewX, AVX 12.1.0, and AVX 12.2.0
- F5 (both LTM and GTM) – version 10.x, 11.x, or 12.x

## Limitations

Not applicable

## Log In to AppViewX



Log in to the AppViewX web interface. The standard format for a login URL is:

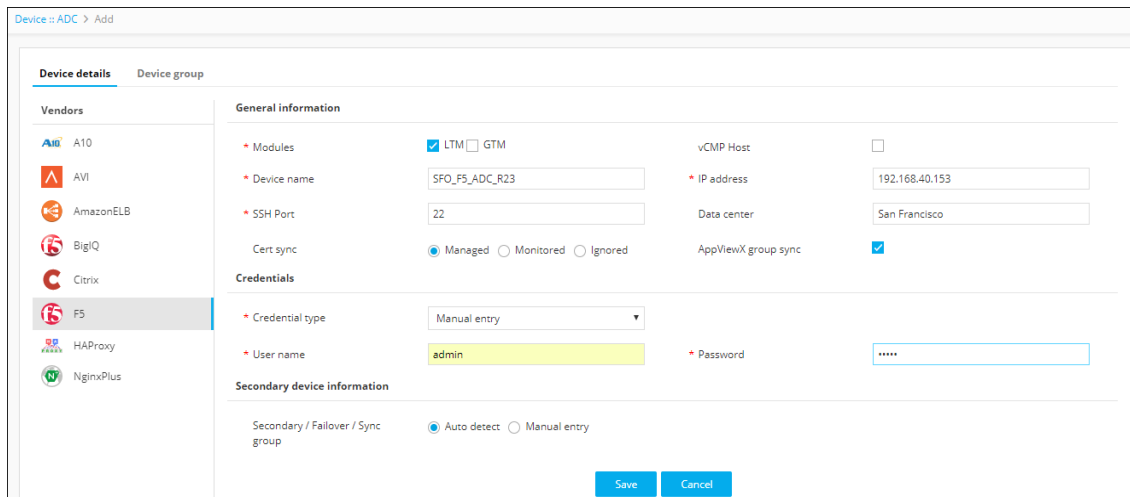
`https://hostname:portnumber.`

The hostname and port number are configured during deployment, with the default port number set to 5004 and the default web credentials set to `admin/AppViewX@123`.

**Note:** It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

## Add an ADC Device: F5 LTM

1. Click the  (Menu) button on the left-hand side of the AppViewX screen.
2. Navigate to **Inventory > Device**.
3. The *Device* screen opens with the **ADC** device inventory displayed by default.
4. Click the  (**Add**) button in the Command bar.
5. On the *Add* screen that opens, click to select **F5** as the ADC vendor.



The screenshot shows the 'Device details' form in the AppViewX interface. The 'Vendors' list on the left includes A10, AVI, AmazonELB, BigIQ, Citrix, F5 (selected), HAProxy, and NginxPlus. The 'General information' section contains the following fields:

- Modules:** LTM (checked), GTM (unchecked)
- Device name:** SFO\_F5\_ADC\_R23
- SSH Port:** 22
- Cert sync:** Managed (selected), Monitored (unchecked), Ignored (unchecked)
- AppViewX group sync:** (checked)
- IP address:** 192.168.40.153
- Data center:** San Francisco
- vCMP Host:** (unchecked)

The 'Credentials' section includes:

- Credential type:** Manual entry
- User name:** admin
- Password:** (masked with asterisks)

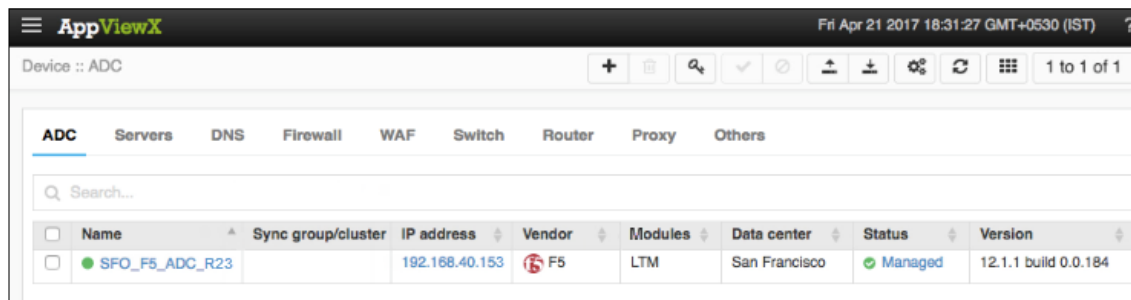
The 'Secondary device information' section has:

- Secondary / Failover / Sync group:** Auto detect (selected), Manual entry (unchecked)

At the bottom right are 'Save' and 'Cancel' buttons.

6. Select the module to be managed on the ADC device.
7. Click the **vCMP Host** check box, if you want to add and manage the vCMP guest devices.
8. In the **Device name** field, enter a name for the devices to help the users identify it.
9. In the **IP address** field, enter the management IP address of the device.
10. Enter the default or custom defined **SSH port** number for the device.
11. (Optional) Specify a **Data center** name in which the device resides and you will have the option later to filter devices based on their location.
12. In the **Cert sync** field, select the radio button for the kind of synchronization relationship you want to establish between SSL certificates on the ADC device and AppViewX: **Managed**, **Monitored**, or **Ignored**.  
**Note:** Ensure that the Cert sync option is in a managed state.
13. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby ADC device.  
**Note:** This is required only in older versions, as the latest versions sync automatically.

14. From the **Credential type** dropdown list, select how to want to provide the credentials:
  - Select **Manual entry**, if you want to manually enter the credential details (user name and the associated password) every time the device is accessed. Select the **Access type** as **API** to help AppViewX to establish communication and to fetch the configuration after the device is in a manage state.
  - Select **Credential list**, if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the [Add a Credential](#) section of this guide.  
When you select the credential name from the dropdown list, the user name and password fields will be auto-filled with the values provided in the credential template.
15. In the **Secondary/Alternate** device field, select how you want to fetch the details of a backup device when the primary device becomes unavailable due to failure or scheduled down time:
  - a. Select **Auto detect** if you want AppViewX to automatically detect and retrieve the configuration of the secondary/alternate device, then click Save to add the device to AppViewX.
  - b. Select **Manual Entry** if you want to manually provide the details of the secondary device. At a minimum, fill in all fields that contain a red asterisk beside their names.
16. Click **Add** to add the secondary device to the list at the bottom of the screen.  
**Note:** You can add more than one secondary devices. The **Update** and **Delete** buttons are enabled only when you try to modify the existing secondary device.
17. Click **Save** to add the new WAF device. The device is then displayed in the table on the WAF tab.



The screenshot shows the AppViewX web interface. At the top, there's a header with the AppViewX logo and a timestamp 'Fri Apr 21 2017 18:31:27 GMT+0530 (IST)'. Below the header, there's a navigation bar with tabs: ADC, Servers, DNS, Firewall, WAF, Switch, Router, Proxy, and Others. The 'WAF' tab is selected. Below the navigation bar, there's a search bar and a table of devices. The table has columns: Name, Sync group/cluster, IP address, Vendor, Modules, Data center, Status, and Version. One device is listed: SFO\_F5\_ADC\_R23, with IP address 192.168.40.153, Vendor F5, Modules LTM, Data center San Francisco, Status Managed, and Version 12.1.1 build 0.0.184.


Name	Sync group/cluster	IP address	Vendor	Modules	Data center	Status	Version
SFO_F5_ADC_R23		192.168.40.153	F5	LTM	San Francisco	Managed	12.1.1 build 0.0.184


The device will display one of the following statuses:

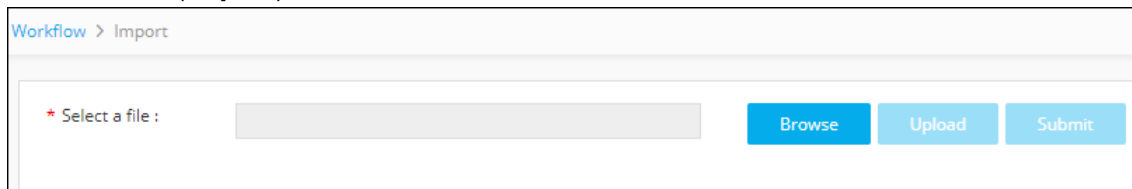
- **In Progress** – Device configuration fetch is in progress.
- **Managed** - Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device, due to invalid login credentials.
- **Failed** – Device configuration fetch failed, due to unsupported version.

## Import Visual Workflows

**Note:** Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

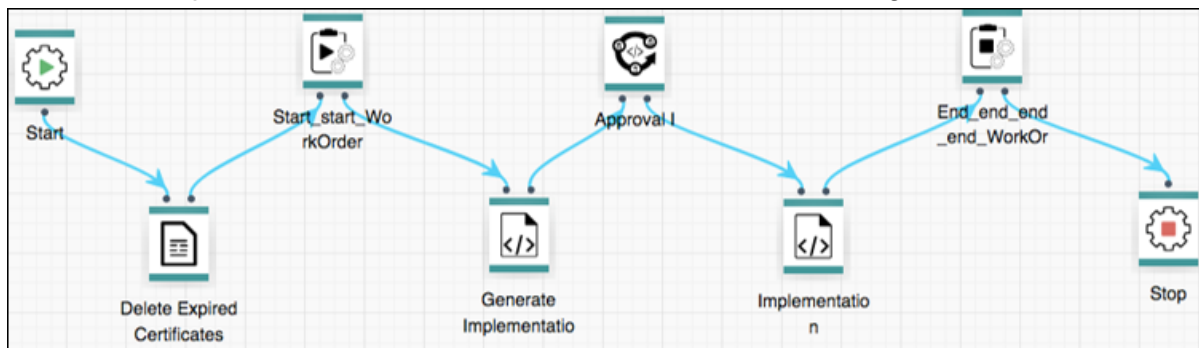
1. Click the  (Menu) button.
2. Navigate to **Workflow > Configurator**.

- Click the  (**Import**) button in the Command bar.





- To import a workflow, complete the following sub-steps:
  - Click the **Browse** button.
  - Select the zip file containing one or more workflows, then click **Upload**.
  - In the table at the bottom of the *Import* page, select the check box beside the unzipped workflow file.
  - Click **Submit** to deploy the workflow into your AppViewX environment.

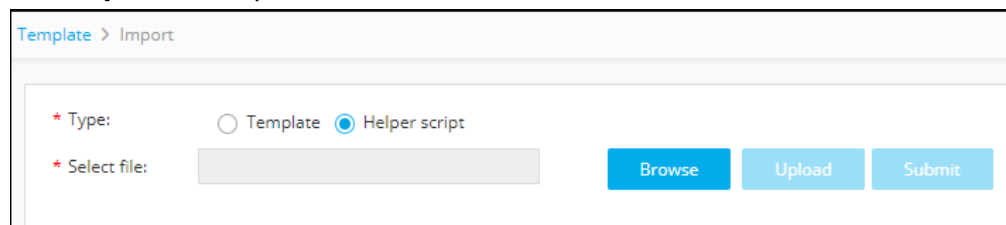
The Delete Expired Certificate from F5 workflow is shown in the image below:



## Import Helper Scripts

**Note:** Free AppViewX comes preloaded with helper scripts. You will only need to use the following import instructions when newer versions of the helper scripts are available.



- Click the  (**Menu**) button.
- Navigate to **Provisioning > Templates**.
- Click the  (**Import**) button in the Command bar.
- On the *Import* screen that opens, complete the following steps:
  - Select the **Helper script** radio button.
  - Click **Browse** and select the helper script zip file you want to import.
  - Click **Upload** to import the file and view its contents.




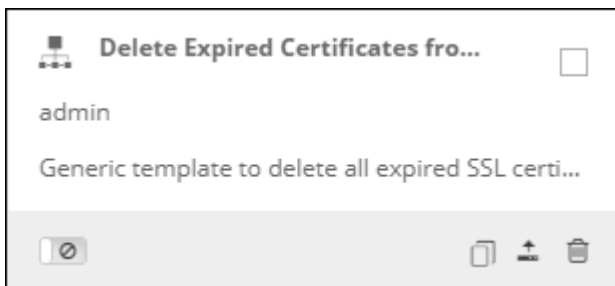
- In the table at the bottom of the *Import* screen, select the check boxes beside each of the helper scripts.
- Click **Submit** to deploy them into your AppViewX environment.

## Enable a Workflow

To enable the Delete Expired Certificates from F5 workflow, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.  
The *Workflow* screen opens.
3. Click the ☐ (**Select**) button on the Delete Expired Certificates from F5 workflow to enable. If the workflow is already selected, a ☒ (**Deselect**) button appears.
4. Click the  (Enable) button in the Command bar.



**Note:** You can also enable the Delete Expired Certificates from F5 workflow from the Card view by clicking the  (**Disable**) button.



5. On the *Confirmation* screen that appears, click **Yes**.

## Delete Expired Certificates from F5 workflow

To submit the Delete Expired Certificates from F5 workflow, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.  
The *Request* screen opens with **My catalog** tab displayed by default. This screen displays all enabled workflows assigned to a specific user role.
3. Click the  (**Run workflow**) button for deleting expired certificates.  
The *Form Builder* screen opens.



Request :: Inventory > Delete Expired Certificates from F5 :: FormBuilder

Search...

Delete Expired Certificates

\* F5 Device

Get F5 Device

Select

\* Expired Cert

Get Expired Cert

None selected

\* Cert and Associated Pr...

Get Profile with Expired Cert

Enter text...

Submit Cancel

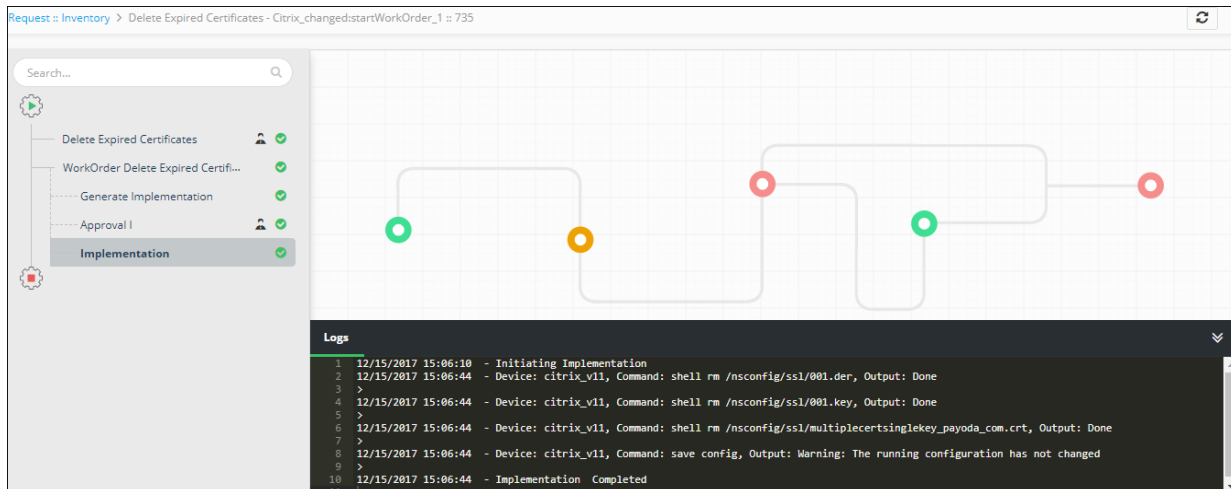
4. Click the **Get F5 Device** button to retrieve the list of F5 devices.
5. From the **F5 Device** dropdown list, select the device from which you want to delete the expired certificates.
6. Click the **Get Expired Cert** button to retrieve the list of expired certificates available on the selected F5 device.
7. From the **Expired Cert** dropdown filed, select the expired certificates you want to delete from the device.
8. Click **Get Profile with Expired Cert** to retrieve the list of client or server profiles to which the certificate and key are associated.
9. In the **Cert and Associated Profile** box, the profiles associated with the certificate and key are displayed.
10. Click **Submit**.

A new **Request ID** is created. To view all requests refer to the [Request Inventory](#) section of this guide.

## WorkOrder flow

The following are the workorder tasks of Delete Expired Certificates from F5 workflow.

**Note:** You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.



1. **Generate Implementation** — The configuration commands are generated in order to delete the expired certificates after associating their SSL profile with the default certificate and key. You can delete those SSL profiles and keys only if they are not associated with any other SSL certificate other than the default certificate.
2. **Approval 1** — Approval of a work order is based on the role assigned to the user (who has an access to approve and implement). After you submit the request form, the configuration changes are reviewed and approved at AppViewX. The configuration changes are implemented on the device only when the approval is received.

The screenshot shows the 'Implementation' form. At the top, there are radio buttons for 'Manual' (selected) and 'Auto'. To the right is a field for 'RFC ID'. Below these are fields for 'Scheduled start date' and 'Scheduled end date'. The main area is divided into two panes, both titled 'expired\_implementation'. The right pane contains a list of commands:

```

1 <device>F5_LON_D1</device>
2 tmsh
3 create cli transaction
4 modify ltm profile client-ssl vs_internetbanking_80 cert default.crt key default.key
5 submit cli transaction
6 delete sys crypto cert yrd.crt
7 delete sys crypto cert 11.4testmigration.crt
8 delete sys crypto key 11.4testmigration.key
9 save sys config
10 quit
11

```

Below the panes is a 'Comments' text area. At the bottom, there are three buttons: 'Implement', 'Reject', and 'Cancel'.

- a. On the screen that opens, select **Manual** or **Auto** radio button depending on how you want to set the implementation process.
- b. If you have selected the **Auto** radio button, fill in all the fields, which are designated by red asterisk (\*) beside their names.
- c. Enter any comments you have related to the implementation request and then, click **Implement**.

3. **Implementation** — The expired certificates and its dependent profiles will be deleted from an F5 device.


## Request Inventory

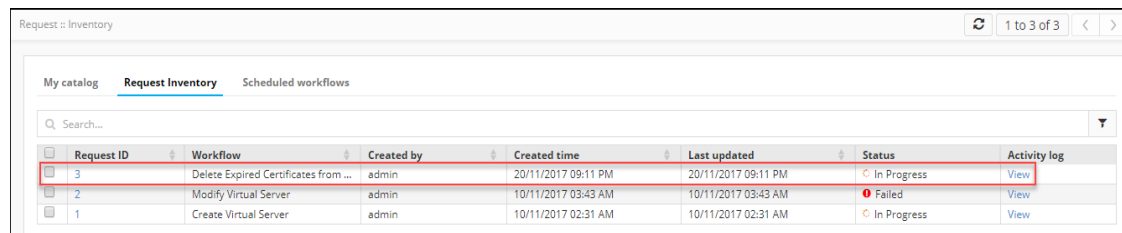
To go to Request inventory, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.


The *Request* screen opens with **My catalog** tab displayed by default.

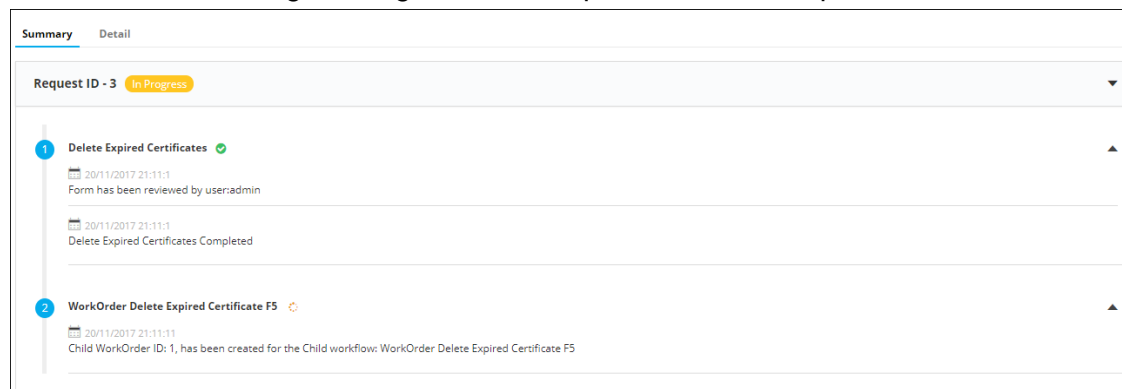
3. Click the **Request Inventory** tab.



This displays all workflows that have been triggered. On the **Request Inventory** screen, you can perform the following tasks: Search for a request using the **Search** field. Click the  (**Filter**) button to select the options you want to use to sort the requests.



Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
3	Delete Expired Certificates from ...	admin	20/11/2017 09:11 PM	20/11/2017 09:11 PM	In Progress	<a href="#">View</a>
2	Modify Virtual Server	admin	10/11/2017 03:43 AM	10/11/2017 03:43 AM	Failed	<a href="#">View</a>
1	Create Virtual Server	admin	10/11/2017 02:31 AM	10/11/2017 02:31 AM	In Progress	<a href="#">View</a>

4. Click the **Request ID** created for Delete Expired Certificates from F5 to view the tasks or phases of a request in a tree-view. For more details, refer to the ([WorkOrder flow](#)) section of this guide.
5. You can also view the following details of the request that are created: request creator, request time, last updated time, status, and activity log.
6. Click **View** in the **Activity log** column to display the request in a stage-view. In the **Summary** tab, click the  (**Expand**) icon to view the details of each task. Click the **Details** tab to view log messages and other particulars of a request.




Request ID - 3	In Progress
1	<b>Delete Expired Certificates</b>  <ul style="list-style-type: none"> <li>20/11/2017 21:11:1</li> <li>Form has been reviewed by user:admin</li> <li>20/11/2017 21:11:1</li> <li>Delete Expired Certificates Completed</li> </ul>
2	<b>WorkOrder Delete Expired Certificate F5</b>  <ul style="list-style-type: none"> <li>20/11/2017 21:11:11</li> <li>Child WorkOrder ID: 1, has been created for the Child workflow: WorkOrder Delete Expired Certificate F5</li> </ul>

## Schedule a Workflow

To schedule a workflow, complete the following steps:




1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.

The *Request* screen opens with **My catalog** tab displayed by default.

3. Click the  (**Schedule workflow**) button on the Delete Expired Certificates from F5 workflow.
4. On the *Delete Expired Certificates from F5* window that opens, select the frequency of the policy migration process: once, hourly, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on what you select.
5. Click **Save**.


## View Scheduled workflows


To go to the scheduled workflow screen, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.
3. The *Request* screen opens with **My catalog** tab displayed by default.
4. Click the **Scheduled workflows** tab.
5. On the Scheduled workflow screen that appears, you can perform the following tasks:
  - a. In the **View log** column, click **View** to display the details of a scheduled workflow.
  - b. Click the  (Pause) or  (Resume) button to temporarily stop or continue the execution of a workflow.

## Add a Credential

To add a credential to a device, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Inventory > Device**.

The *Device* screen opens with the **ADC** tab selected by default.
3. Click the **ADC** tab.
4. Click the check box beside the device name, then click the  (**Credential**) button in the Command bar.
5. On the *Add credential* screen that appears, enter the name of the credential you want to add to the device.
6. Enter the **username** and **password** associated with the credential.
7. (Optional) If a secondary credential password was created by a vendor in order to communicate with the device, thus allowing different levels of control over the credential, enter this password in the **Secondary password** field.
8. Click **Save**.

The credential is then added to the table at the bottom of the screen. You can delete a credential or modify its name, user name, or password by selecting the check box beside the credential name in the table at the bottom of the screen and then clicking either the **Modify credential** or **Delete** button in the Command bar.

## Troubleshooting

### **I cannot find the Delete Expired Certificates from F5 workflow in the Request Catalog**

You must enable the workflow from the Configurator section. For more details on how to enable a workflow, refer to the [Enable a Workflow](#) section of this guide.

### **Why is the ASM policy not migrated to the target device?**

You must have an Admin user privileges in order to add an F5 device in the AppViewX inventory. For more details on how to add an ADC device, refer to the [Add an ADC Device: F5 LTM](#) device section of this guide.