



Move Faster

Reduce Cost

Eliminate Errors

AFM Policy Creation Workflow Guide

Copyright © 2018 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).

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

This product includes software developed by the VMware (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

Web: www.appviewx.com

Document Information

Software Version: 12.2.0

Document Version: 1.0

Last updated on: February 20, 2018

Contents

Description	1
Prerequisites	1
Compatible Software Versions	1
Limitations.....	1
REST API	1
Log In to AppViewX	2
Import Visual Workflows.....	2
Import Helper Scripts	2
Enable the AFM Policy Creation Workflow	3
Add a Firewall Device: F5 LTM	3
Add a Server	5
AFM Policy Creation Workflow	6
WorkOrder Flow.....	9
Request Inventory.....	10
Schedule a Workflow	11
View Scheduled Workflows	11
Add a Credential	12
Troubleshooting	12

Description

The AFM Policy Creation workflow creates an AFM rule and pushes it to an active AFM policy in the F5 BIG-IP devices. The policies available within the selected partitions of an F5 device will be listed. It provides an option to select the policy (for which a rule needs to be created) and define source and destination addresses with the Geo-location and Fully Qualified Domain Name (FQDN). Also, the sequence, logging, and status of the created AFM rule can be define using this workflow.

The flow diagram for the AFM Policy Creation workflow 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 have been added in the AppViewX inventory and assigned to a data center.
- Each ADC device is a managed entity in AppViewX.
- The DNS resolver has been configured in the F5 device.
- The AFM module has been enabled in the device.

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 11.x and 12.x

Limitations

Not applicable.

REST API

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`.

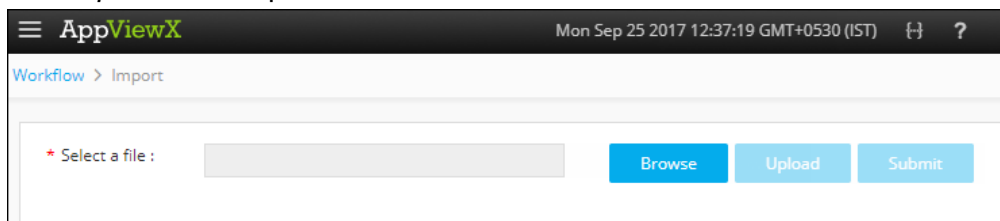
Note: It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

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.

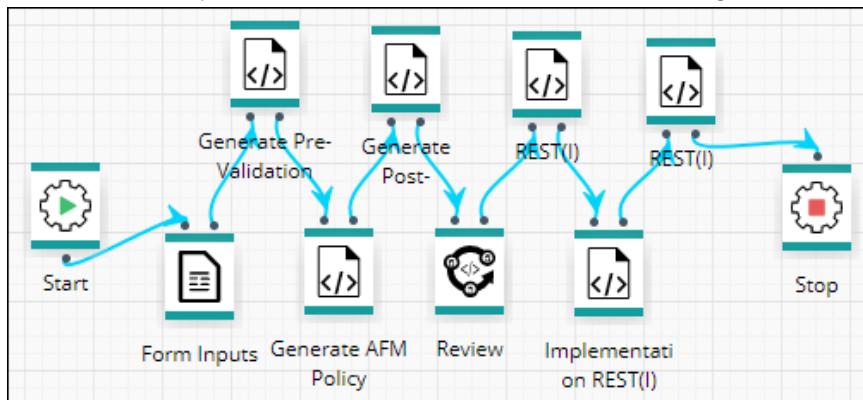
1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. Click the  (**Import**) button in the Command bar.

The *Import* screen opens.





4. Click the **Browse** button.
5. Select the zip file containing one or more workflows, then click **Upload**.
6. In the table at the bottom of the Import page, select the check box beside the unzipped workflow file.
7. Click **Submit** to deploy the workflow into your AppViewX environment.

The AFM Policy Creation workflow is shown in the image below:

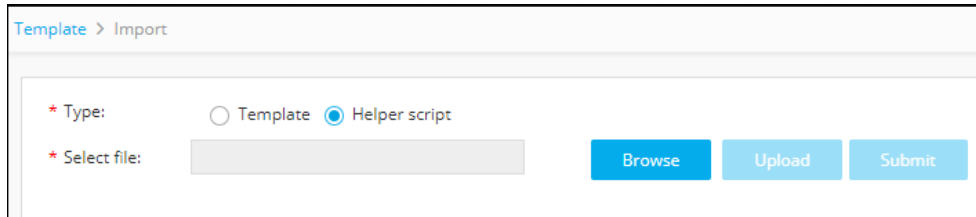


Import Helper Scripts

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.

1. Click the  (**Menu**) button.
2. Navigate to **Provisioning > Templates**.
3. Click the  (**Import**) button in the Command bar.





An *Import* screen opens.



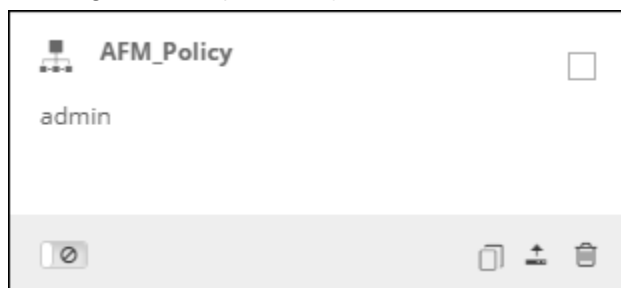
4. Select the **Helper script** radio button.
5. Click **Browse** and select the helper script zip file you want to import.
6. Click **Upload** to import the file and view its contents.
7. In the table at the bottom of the *Import* page, select the check box beside each of the helper scripts.
8. Click **Submit** to deploy them into your AppViewX environment.

Enable the AFM Policy Creation Workflow

To enable the AFM Policy Creation 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 **AFM Policy Creation** 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 AFM Policy Creation workflow from the Card view by clicking the  (**Disable**) button.




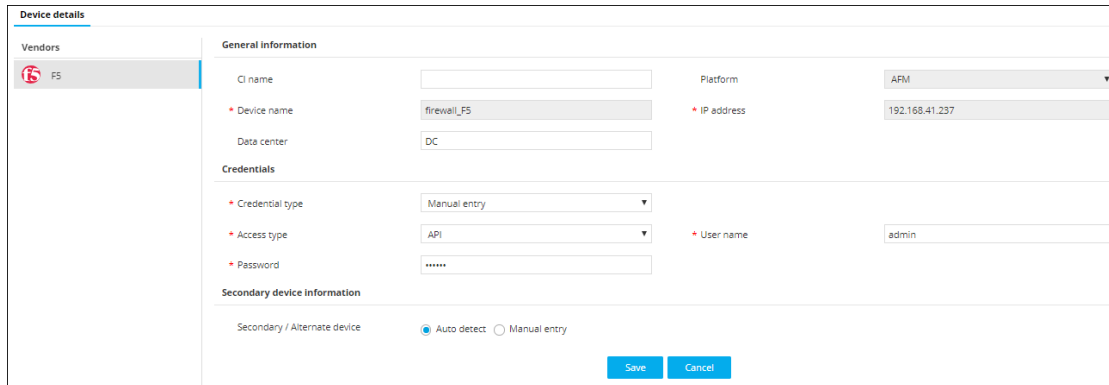
5. On the *Confirmation* screen that appears, click **Yes**

Add a Firewall Device: F5 LTM

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

The *Device* screen opens with the **ADC** tab displayed by default.

3. Click the **Firewall** tab.
4. Click the  (**Add**) button in the Command bar.
5. On the *Add* screen that opens, click to select **F5** as the vendor.



6. In the CI name field, enter the asset number of the device that is used in provisioning.
7. Select the platform supported for the F5 vendor from the dropdown list.
8. Enter a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
9. Enter the **management IP address** of the device.
10. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
11. From the **Credential type** dropdown list, select how you want to provide the credentials:
 - a. Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.
 - b. 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 are auto-populated with the values provided in the credential template.
12. 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.
13. Click **Add** to add the secondary device to the list at the bottom of the screen.

Note: You can add more than one secondary device. The **Update** and **Delete** buttons are enabled only when you try to modify existing secondary devices.

14. Click **Save** to add the new Firewall device. It will then appear in the table on the Firewall tab.


ADC Server DNS Firewall WAF Switch Router Proxy Cloud Others								
Search...								
<input type="checkbox"/>	Name	Policy name	IP address	Data center	Status	Vendor	Platform	Credential type
<input checked="" type="checkbox"/>	AFM_F5		192.168.41.237		Managed	F5	AFM	Manual entry
<input type="checkbox"/>	55.31		192.168.55.31	dc	Unresolved	Juniper	SRX	Manual entry
<input type="checkbox"/>	ckp_55.214		192.168.55.214	dc	Unresolved	CheckPoint	Security Manag...	Manual entry
<input type="checkbox"/>	dev175		192.168.175.1		Unresolved	Cisco	ASA	Manual entry

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.

Add a Server

To add a server, complete the following steps:

1. Click the  (**Menu**) button on the left-hand side of the AppViewX screen
2. Navigate to **Inventory > Device**.

The *Device* screen opens with **ADC** tab displayed by default.


3. Click the **Server** tab.
4. Click the  (**Add**) button in the Command bar.


The *Add* screen opens, with the **APACHE** tab selected by default.


5. Click to select **Other Devices** and add the DNS Name Server.


Device details


Vendors











Server details

Server type

Other devices

Server name

IP address

Data center

Credentials

Credential type

Manual entry

User name

Password

Save

Cancel

6. In the **Server name** field, enter a name for the server to help users identify it.
7. In the **IP address** field, enter the IP address for which the connection must be established.
8. (Optional) In the **Data center** field, enter the data center name in which the device resides.
9. 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 **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. After you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
10. Click **Save**. A new server is added to the AppViewX inventory and appears on the *Server* tab.

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.




AFM Policy Creation Workflow



To submit the AFM Policy Creation 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 from the Card view of the AFM Policy Creation workflow.

The *Form Builder* screen opens.

* Device Version	v11	
* Select Device	Select	
* Select Partition	Select	
* Rule Name		
Description		
* Available Policy-Context	Select	
* Source address	<input checked="" type="radio"/> any <input type="radio"/> Other	
Vlan Name	None selected	
Tunnel Name	None selected	
* Destination address	<input checked="" type="radio"/> any <input type="radio"/> Other	
* Protocol	<input checked="" type="radio"/> tcp <input type="radio"/> udp <input type="radio"/> Other	

4. Select the version of the F5 device from the list of supported versions that are populated.
5. In the **Selected Device** field, click the  (**Retrieve field values**) button to fetch the list of available F5 devices based on the version you selected. Select the F5 device on which you want to create and add a rule to the AFM policy.
6. In the **Selected Partition** field, click the  (**Retrieve field values**) button to fetch the list available partitions on the selected device and select the required partition from the dropdown list.
7. Enter a name for the rule that you want to create.
8. (Optional) In the **Description** field, enter any additional information required for the AFM rule.
9. In the **Available Policy-Context** field, click the  (**Retrieve field values**) button to fetch the list of active policies available in the selected F5 device and select the required policy on which the AFM rule has to be created.
10. Depending on whether or not you want to provide the **Source address** details, select the **any** or **Other** radio button.
 - a. Select **any** if you want the rule to be applicable for any of the source address.
 - b. Select **others** if you want the rule to be applicable for a particular source address and then, complete the following fields:
 - i. Enter a name for the Source address list to help the users identify it.
 - ii. Enter the IP address, geographical location, and FDQN of the source address you trying to configure.

11. In the **Vlan Name** field, click the  (**Retrieve field values**) button to fetch the list of VLAN connections and select the required connection which you want to establish.
12. In the **Tunnel Name** field, click the  (**Retrieve field values**) button to fetch the list of available protocols and select the protocol for the secure movement of information from the source address to the destination address.
13. Depending on whether or not you want to provide the **Destination address** details, select the **any** or **Other** radio button.
 - a. Select **any** if you want the rule to be applicable for any of the destination address.
 - b. Select **others** if you want the rule to be applicable for a particular destination address and then, complete the following fields:
 - i. Enter a name for the destination address list to help the users identify it.
 - ii. Enter the IP address, geographical location, and FDQN of the destination address you trying to configure.
14. In the **Protocol** field, select one of the following protocols you want to use:
 - a. Select **tcp** or **udp** radio button based on the type of connection you want to establish for the data transmission.
 - b. Select **Other** if you want to establish a connection using any particular protocol and then, enter a name or number for the protocol to help the users identify it.
15. If you have selected the protocol type tcp or udp then, enter the port name and port number for the source and destination address in their corresponding fields.
16. From the **Status** dropdown list, select the policy status that you want to be displayed.

* Status	enabled	▼
* Action	accept	▼
* Logging	yes	▼
* Order	place-before	▼
* In-Depth Order	last	▼

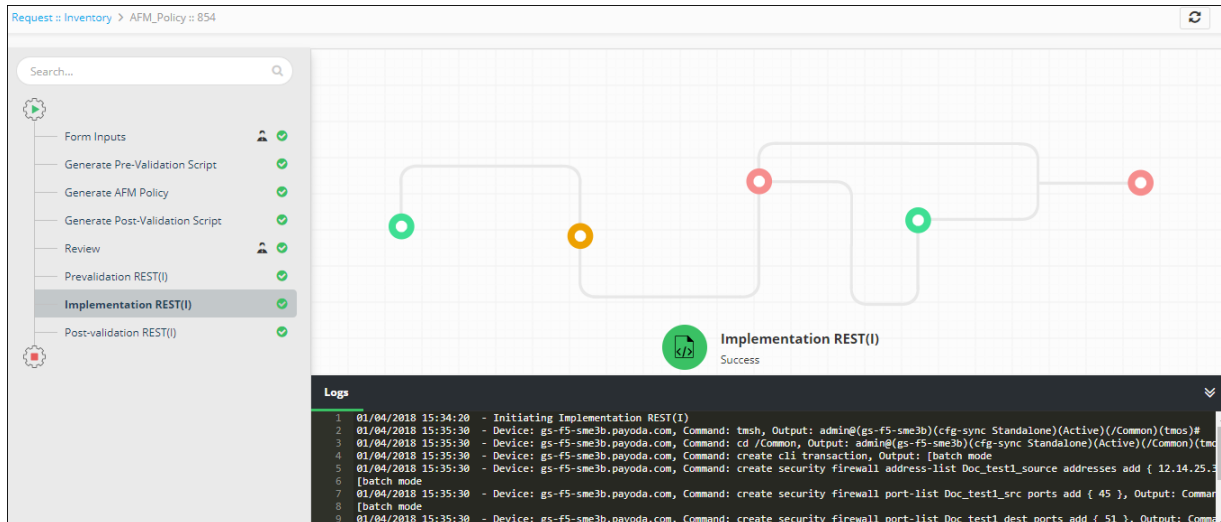
17. From the **Action** dropdown list, select the action you want the rule to perform.
18. Depending on whether or not you want to log the events, select the option **Yes** or **No** from the dropdown list.
19. Select the sequence in which you want the rule to be placed in the AFM policy from the **Order** and **In-depth Order** fields respectively.
20. Click **Submit**.

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

WorkOrder Flow

The following are the workorder tasks for the AFM Policy Creation 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.



- **Generate Pre-Validation Script** — Configuration commands are generated to initiate the pre-validation process.
- **Generate AFM Policy** — Configuration commands are generated to create and add a rule to the AFM policy.
- **Generate Post-Validation Script** — Configuration commands are generated to initiate the post-validation process.
- **Review** — After you submit the request form, the configuration changes are reviewed at AppViewX. The configuration changes are implemented on the device only after it is reviewed.

Postvalidation	Implementation Script
Prevalidation	
Implementation Script	<pre> 1 <device>gs-f5-sme3b.payoda.com</device> 2 tmsb 3 cd /Common 4 create cli transaction 5 create security firewall address-list Doc_test1_source addresses add { 12.14.25.36 } fqdns add { 6 create security firewall port-list Doc_test1_src ports add { 45 } 7 create security firewall port-list Doc_test1_dest ports add { 51 } 8 modify security firewall policy test rules add { Doc_test1 { ip-protocol tcp source { address 9 submit cli transaction 10 quit 11 </pre>
Comments	test
<div>Implement Reject Cancel</div>	

- **Prevalidation** — Checks if the rule you want to create is available in the AFM policy.

- **Implementation** — A new rule is created and pushed to an active AFM policy in the F5 BIG-IP device and also, it is applied to the source and destination addresses based on the inputs provided in the form fields.
- **Post-Validation** — Checks if the rule is successfully created and pushed to the AFM policy.

Request Inventory


To go to the 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 search for a request using the **Search** field and/or click the  (**Filter**) button to select the options you want to use to sort the requests.

My catalog Request Inventory Scheduled workflows							
Q Search...							
Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log	
864	Delete Expired Certificates - Citrix	admin	05/01/2018 02:41 PM	05/01/2018 02:41 PM	In Progress	View	
863	Role_Dashboard_Automation_V2	admin	04/01/2018 09:07 PM	04/01/2018 09:07 PM	Failed	View	
862	Role_Dashboard_Automation_V2	admin	04/01/2018 09:05 PM	04/01/2018 09:05 PM	Failed	View	
861	Role_Dashboard_Automation_V2	admin	04/01/2018 09:05 PM	04/01/2018 09:05 PM	Failed	View	
860	Role_Dashboard_Automation_V2	admin	04/01/2018 08:35 PM	04/01/2018 08:35 PM	Completed	View	
859	Role_Dashboard_Automation_V2	admin	04/01/2018 08:32 PM	04/01/2018 08:32 PM	Completed	View	
858	Role_Dashboard_Automation_V2	admin	04/01/2018 08:05 PM	04/01/2018 08:05 PM	Failed	View	
857	Role_Dashboard_Automation_V2	admin	04/01/2018 08:00 PM	04/01/2018 08:00 PM	In Progress	View	
856	Role_Dashboard_Automation_V2	admin	04/01/2018 07:49 PM	04/01/2018 07:49 PM	In Progress	View	
855	AVX_GS_84548_Push_Renewed_...	admin	04/01/2018 05:59 PM	04/01/2018 05:59 PM	In Progress	View	
854	AFM_Policy	admin	04/01/2018 03:31 PM	04/01/2018 03:31 PM	Completed	View	

4. Click the **Request ID** created for AFM Policy Creation 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 was 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 :: Inventory > AFM_Policy : 854 : log

Summary Detail

Request ID - 854 Completed

1 Form Inputs ✓

4/1/2018 15:31:52
Form has been reviewed by user:admin

4/1/2018 15:31:52
Form Inputs Completed

2 Generate Pre-Validation Script ✓



4/1/2018 15:31:58
Initiating Generate Pre-Validation Script

4/1/2018 15:32:10
Config generated successfully

4/1/2018 15:32:18
Generate Pre-Validation Script Completed


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 the **My catalog** tab displayed by default.
3. Click the  (**Schedule workflow**) button on the AFM Policy Creation workflow.
4. On the AFM Policy Creation 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 the **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:
 - In the **View log** column, click **View** to display the details of a scheduled workflow.

- 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 **WAF** 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 AFM Policy Creation 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 the AFM Policy Creation Workflow](#) section of this guide.

I cannot retrieve the Virtual Server details

The F5 AFM devices should be added under Firewall section in the AppViewX inventory. For more details on how to add a device, refer to the [Add a Firewall Device: F5 LTM](#) section of this guide.