

ASM 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: January 05, 2018

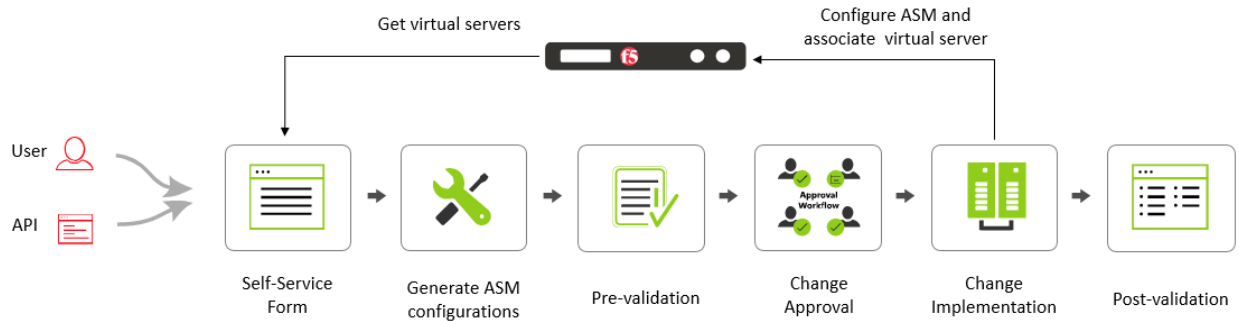
Contents

Description	1
Prerequisites	1
Compatible Software Versions	1
Log In to AppViewX.....	1
Import Visual Workflows.....	1
Import Helper Scripts	2
Enable a Workflow	3
Add an ADC Device: F5	3
Add a Web Application Firewall (WAF): F5 LTM.....	5
ASM Policy Creation Workflow	7
WorkOrder flow	9
Request Inventory	10
Schedule a Workflows.....	11
View Scheduled Workflows	11
Add a Credential	12
Troubleshooting	12

Description

The “ASM Policy Creation” workflow is used to create ASM policies in an F5 device. The new ASM policy can be associated with multiple virtual servers.

The flow diagram of ASM Policy Creation workflow is shown in the image below:



Prerequisites

To run this automation template, ensure that the following pre-requisites are met:

- The F5 devices must be added and managed under the ADC and WAF category in AppViewX inventory.
- The Virtual Servers must have HTTP profiles associated with them.

Compatible Software Versions

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

- AVX 12.2.0
- F5 (both LTM and GTM) – version 11.6 and later

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.

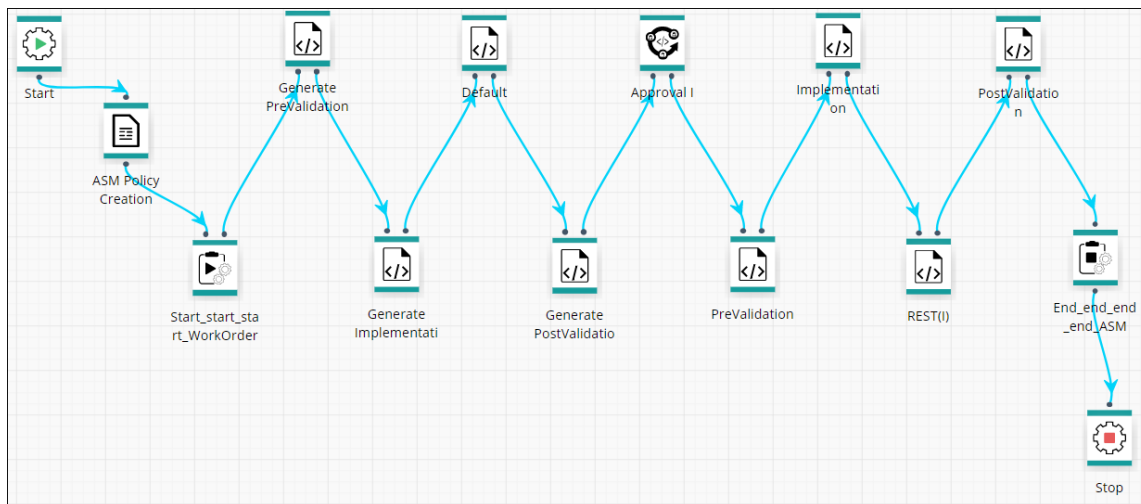
Import Visual Workflows

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.



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

The ASM Policy Creating 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.
4. On the *Import* screen that opens, complete the following steps:
 - a. Select the **Helper script** radio button.
 - b. Click **Browse** and select the helper script zip file you want to import.
 - c. Click **Upload** to import the file and view its contents.

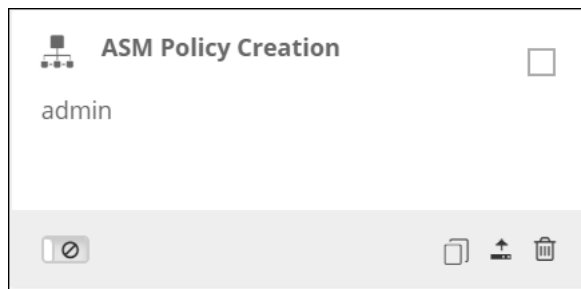
- d. In the table at the bottom of the Import page, select the check boxes beside each of the helper scripts.
- e. Click **Submit** to deploy them into your AppViewX environment.

Enable a Workflow

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



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

Add an ADC Device: F5

1. Click the  (Menu) button.
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.

6. Select the module to be managed on the ADC device.
7. Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
8. Enter the **management IP address** of the device.
9. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
10. 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**.
11. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby F5 ADC device. This is required in older F5 versions like v10. The latest versions of F5 sync automatically.
12. Select a **Credential type** from the dropdown menu.
13. Enter the **User name** and **Password** that are associated with the credentials.
Note: The user you enter in the **User name** field must have advanced shell access.
14. Select **Auto detect** to automatically detect and add secondary or failover devices or sync groups to the ADC device inventory.
15. Click **Save** to save the new ADC device in the table on the ADC tab.



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

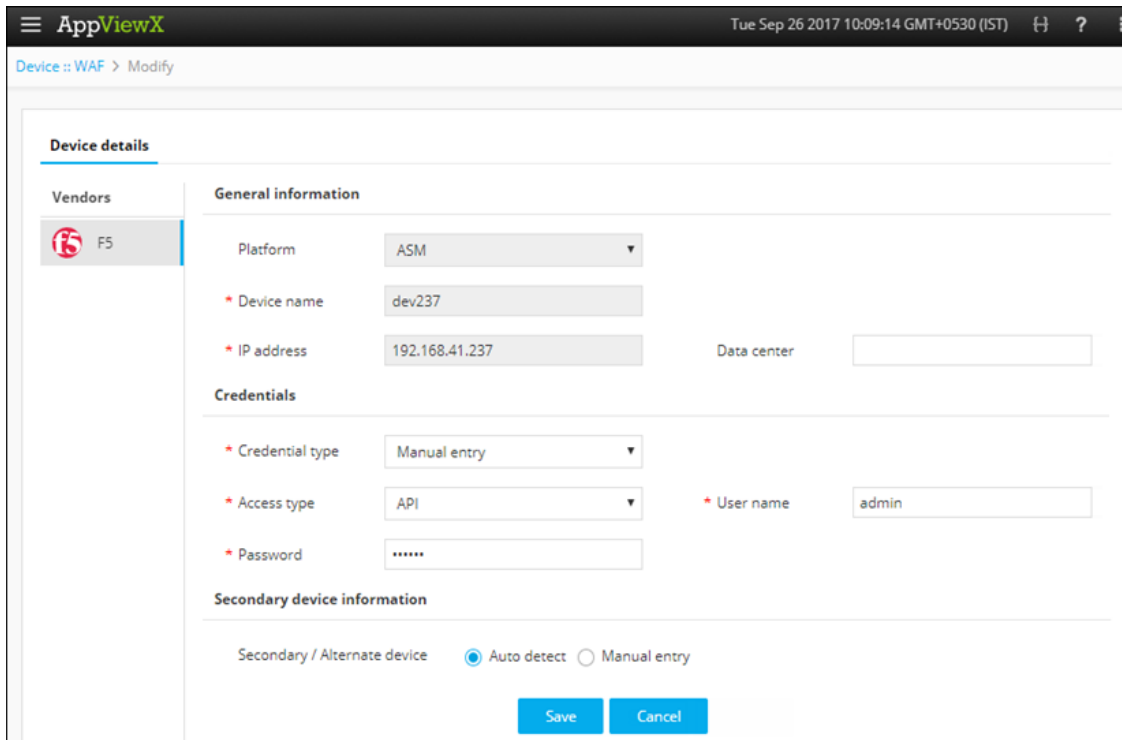
The device will display one of the following statuses:

- **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.

Add a Web Application Firewall (WAF): F5 LTM

1. Click the  (**Menu**) button.
2. Navigate to **Inventory > Device**.
3. The *Device* screen opens with the **ADC** device inventory displayed by default.
4. Click the **WAF** tab.
5. On the *WAF inventory* screen that opens, click the  (**Add**) button in the Command bar.



AppViewX Tue Sep 26 2017 10:09:14 GMT+0530 (IST)

Device :: WAF > Modify

Device details

Vendors

F5

General information

Platform: ASM

* Device name: dev237

* IP address: 192.168.41.237 Data center:

Credentials

* Credential type: Manual entry

* Access type: API * User name: admin

* Password:

Secondary device information

Secondary / Alternate device: ☒ Auto detect ☐ Manual entry

Save Cancel

6. In the right-hand column on the *Add* screen that appears, enter the following details to add a device of an F5 vendor:
 - a. From the **Platform** dropdown list, select the platform as **ASM** (Application Security Manager).
 - b. In the **Device name** field, enter a name for the primary device to help users identify it in the network.
 - c. In the **IP address** field, enter the IP address of a device for which the connection must be established.
 - d. (Optional) In the **Data center** field, enter the name of the data center in which the network device resides.
 - e. From the **Credential type** dropdown list, select how you 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 are auto-populated with the values provided in the credential template.
- f. 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:
 - 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.
 - 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.
- g. 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.
- h. Click **Save** to add the new WAF device. The device is then displayed in the table on the WAF tab.

Name	Access type	IP address	Vendor	Policy count	Data center	Version	Status	P
dev214	API	192.168.40.214	F5	0			Failed	A
dev237	API	192.168.41.237	F5	12		11.5.3	Managed	A

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.

ASM Policy Creation Workflow


To submit the ASM 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 on the ASM Policy Creation, the respective Form Builder screen opens.
 4. Click the **Get Device List** button to retrieve the LTM devices present in the AppViewX inventory. The retrieved list will be populated in the **Device List** dropdown list.
 5. From the **Device List** dropdown, search for or select the preferred device.
 6. In the **Policy name** field, enter a name for the ASM policy that you want to create.
 7. In the **Description** field, provide a description for your ASM policy.
 8. From the **Partitions** dropdown list, select the partition in the F5 device in which the ASM policy must reside.
 9. From the **Auto Policy Builder** dropdown list, select **Enable** or **Disable**.
 10. From the **Predefined Template** dropdown list, select the existing template in Provisioning, using which the ASM policy must be created.
 11. From the **Enforcement Mode** dropdown list, select the method (Transparent or Blocking) which must be used to handle the violations.
 12. In the **Enforcement Readiness Period (Days)** field, enter the number of days up to which the enforcement is applicable.
 13. From the **Encoding method** dropdown list, select the encryption method to be used in the ASM policy.
 14. Click the **Get Virtual Server(s)** button to retrieve the virtual servers present in the AppViewX inventory.
 15. From the Virtual Server(s) dropdown list, select the preferred virtual server.
 16. In the **Source filter - Whitelist IP/Mask** field, enter the IP addresses that must be whitelisted or masked. After entering each IP, you must click  to add them to the **Whitelist/Mask IP list**.
18. For the **Add the features to be enabled/configured for the policy** field, select **Yes** or **No**. Then, complete the following steps depending on whether or not you want to configure a field:

Note: You also have an option to edit, reset, and delete the details provided.

- a. For the **Vulnerability Tool** field, select **Yes** to check for any vulnerabilities in the Website to which the ASM policy is associated. Then, select the preferred tool from the **Vulnerability Tool Names** dropdown list.
- b. For the **Sensitive Parameters** field, select **Yes** to enter the keywords which must be allowed through the ASM policy. After entering each keyword in the **Sensitive Parameters** field, you must click  to add them to the **Sensitive Parameter List**.

Note: You also have an option to edit, reset, and delete the details provided.

- c. For the **XML Profile** field, select **Yes** to validate the XML request to the Website. Then, complete the following steps:
 - i. In the **XML Profile name** field, enter a name for the XML profile.

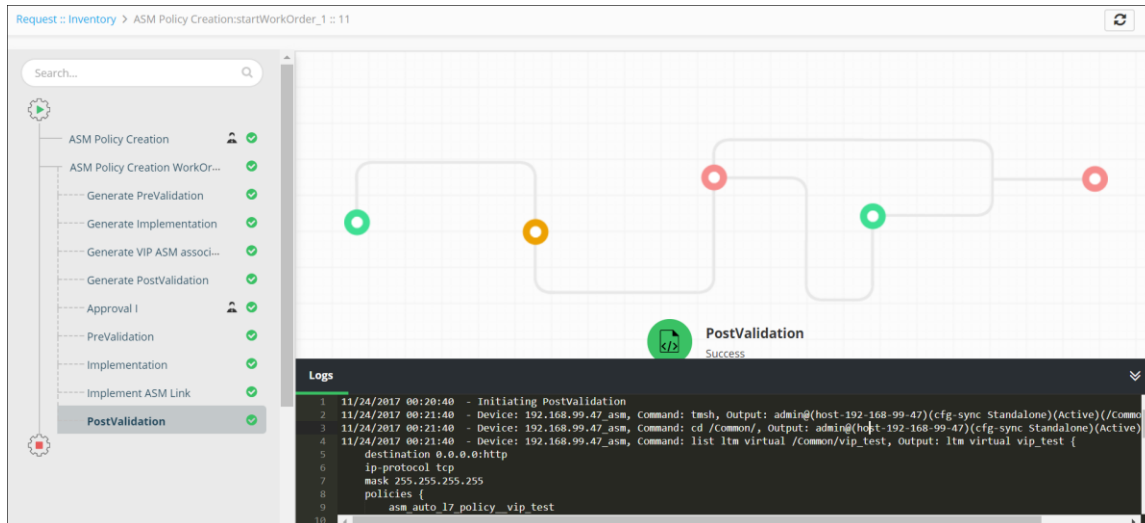
- ii. Select **Yes** or **No** depending on whether or not you want to check if the digital signatures in your XML are in compliance with the World Wide Web Consortium (W3C) standards.
 - iii. From the **Defence Level** dropdown list, select the extent of protection you want against the attacks.
- d. For the **JSON Profile** field, select **Yes** to validate the JSON request to the Website. Then, complete the following steps:
 - i. In the JSON Profile name field, enter a name for the JSON profile.
 - ii. Select **Yes** or **No** depending on whether or not you want to check if the digital signatures in your JSON are in compliance with the World Wide Web Consortium (W3C) standards.
 - iii. Fill in all the mandatory fields.
- e. For the **GWT Profile** field, select **Yes** to check the presence of incorrect data in the request to the Website. Then, fill in all the mandatory fields.
- f. For the **Cookies** field, select **Yes** to validate the cookies from the client to the Website. Then, fill in all the mandatory fields.
- g. For the **Allowed Headers** field, select **Yes** to ensure that all the requests to the Website are prefixed with HTTP or HTTPS.
- h. For the **File Type** field, select **Yes** to configure the type of files you want to allow and block.
- i. For the **URL** field, select **Yes** to configure the type of application protocol you want to use for the Website.
- j. For the **Web Scraping** field, select **Yes** to enable or disable the notifications upon various activities on the Website.
- k. For the **Signature Sets** field, select **Yes** to retrieve and use the list of signatures that contain various patterns to detect the attacks.
- l. For the **Data guard for Credit Card Number** field, select **Yes** to protect the credit card details.
- m. For the **Data guard for Social Security Number** field, select **Yes** to protect the social security card details.
- n. For the **Brute Force Attack Prevention** field, select **Yes** to prevent the trial and error methods by application programs to decode the encrypted data.
- o. For the **CSRF** field, select **Yes** to prevent the Cross-Site Request Forgery attacks.
- p. For the **IP address Intelligence** field, click **Yes** to block the unwanted IPs from accessing the Website.
- q. For the **Redirection Protection** field, click **Yes** to prevent the Website from being redirected to malicious Websites.
- r. For the **Login Enforcement** field, click **Yes** to use the valid credentials to log in to the Website.
- s. For the **Session Awareness** field, click **Yes** to detect the IP addresses instigating attacks on the Website.

19. Click **Submit** to trigger the workflow immediately.

WorkOrder flow

Following are the workorder tasks of ASM 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.



1. **Generate Prevalidation** — Configuration commands are generated to initiate the policy prevalidation process.
2. **Generate Implementation** — Configuration commands are generated to initiate the implementation process.
3. **Generate VIP ASM association** — Configuration commands are generated to initiate the association of the VIP with ASM policy.
4. **Generate PostValidation** — Configuration commands are generated to initiate the post validation process.
5. **Approval I** — You can review the configuration commands generated in steps 1-4 in the respective tabs.
6. **Prevalidation** — Checks if the selected virtual servers exist.
7. **Implementation** — The ASM policy is created with the selected features.
8. **Implement ASM Link** — The ASM policy is associated with the selected virtual servers.
9. **PostValidation** — Check if the ASM policy is associated with the selected virtual servers.

Prevalidation	Implementation <pre> 1 <device>asm2469</device> 2 tmsb 3 cd /Common/ 4 create asm policy testing_asm_policy_nov_2 active blocking-mode disabled policy-builder 5 save sys config 6 quit 7 <rest> 8 <url>https://172.16.24.69/mgmt/tm/asm/policies?filter=name%20eq%20testing_asm_policy_n 9 <type>GET</type> 10 <header>{"Authorization": "Basic YWRtaW46U3VwM3JtQG4=", "Content-Type": "application/js 11 <request_entity>{"Content-Type": "application/json", "Accept": "application/json"}</req 12 <response_parse_type>json</response_parse_type> 13 <response_param>hash_code=items/id</response_param> 14 </rest> 15 16 <rest> 17 <url>https://172.16.24.69/mgmt/tm/asm/policies/\$hash_code\$\$whitelist-ips</url> 18 <type>POST</type> 19 <header>{"Authorization": "Basic YWRtaW46U3VwM3JtQG4=", "Content-Type": "application/js 20 21 </pre>
Postvalidation	
Implementation asm link	
Implementation	
Comments	

[Cancel](#)


Request Inventory





To go to the Request inventory, complete the following steps:


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

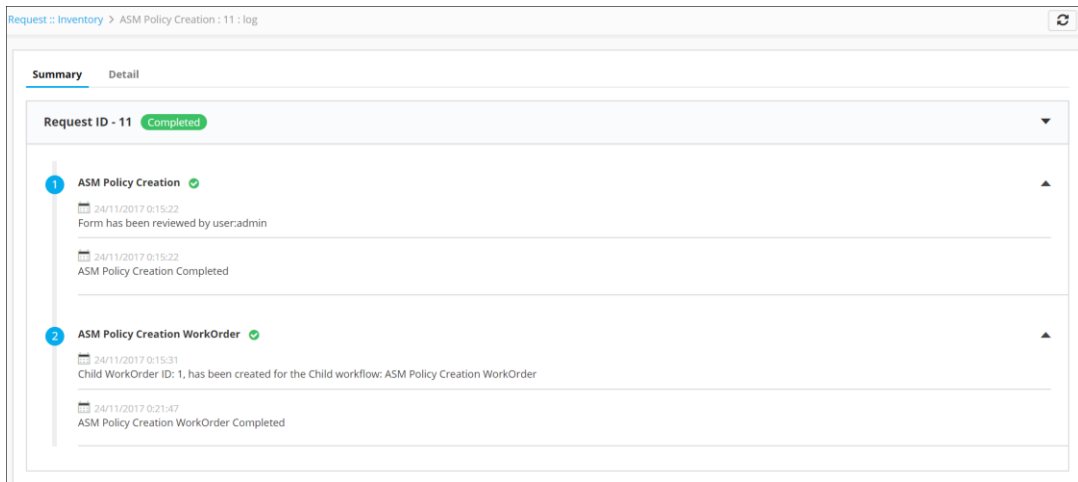
The *Request* screen opens with **My catalog** tab displayed by default.

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	
 129	ASM Policy Creation	admin	02/11/2017 06:19 PM	02/11/2017 06:19 PM	 Completed	View	

4. Click the **Request ID** created for ASM 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 are created: request creator, request time, last updated time, status, and activity log.
6. Click the **View** link 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.






Schedule a Workflows

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 ASM Policy Creation workflow.
4. On the ASM 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 **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 **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 ASM 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 a Workflow](#) section of this guide.