



Move Faster

Eliminate Errors

Reduce Cost

ASM Policy Migration

October 2017

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).

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 (212) 400 7541

Tel: +44 (0) 203-514-2226

Email: info@appviewx.com

Web: <http://www.appviewx.com>

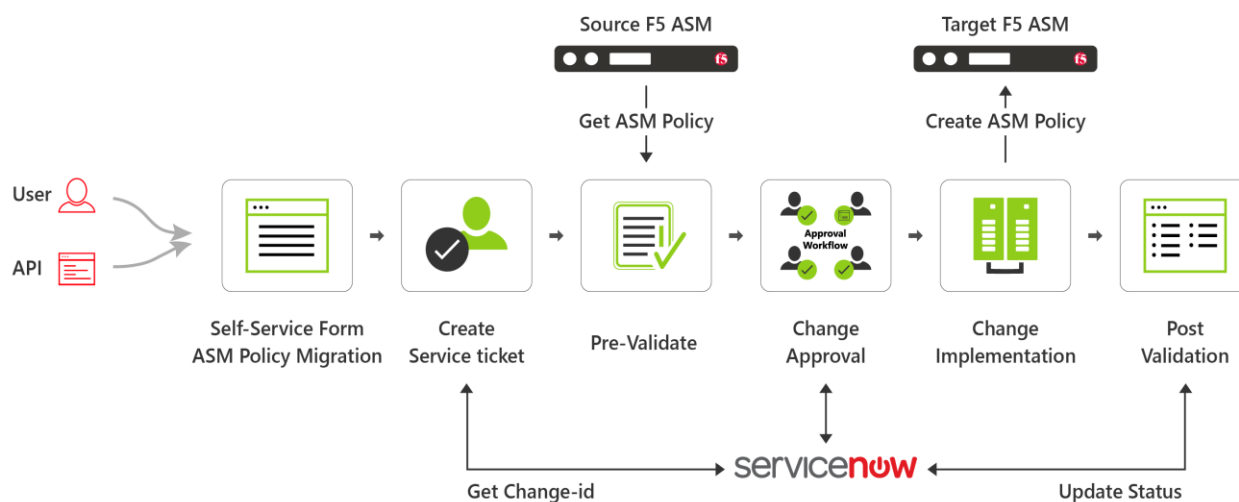
Contents

Description	1
Prerequisites.....	1
Compatible Software Versions.....	1
Limitations	2
Log In to AppViewX.....	2
Add a Web Application Firewall (WAF): F5 LTM	2
Add an ADC Device: F5 LTM.....	4
Register an ITSM Device: ServiceNow	5
Import Visual Workflows	6
Import Helper Scripts	6
Enable a Workflow	7
ASM Policy Migration workflow	7
WorkOrder flow	8
Request Inventory	11
Schedule a Workflow	12
Scheduled workflows	12
Add a Credential	12
Troubleshooting	13

Description

The ASM Policy Migration workflow is used for migrating ASM policies between the F5 devices (that is from a source device to a destination device). You can only migrate the policy from a lower version of F5 device to a higher version or between the same versions of F5 devices. A new policy is created on the destination device with the same configuration as in the source device and is associated to a virtual server present in the destination device. Also, you have an option to integrate the workflow with an ITSM tool – ServiceNow for approvals and tracking. The ServiceNow change request ID is associated with the request and is updated based on the implementation status.

The ASM Policy Migration 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 is downloaded and installed.
- The ADC devices must have been added in the AppViewX inventory with a Data center name.
- The F5 ASM devices should be added under both WAF and ADC sections in the AppViewX inventory.
- Each ADC device must be a managed entity in AppViewX.
- Add a device in AppViewX inventory with the admin user privileges.
- An ITSM tool (ServiceNow), must have been configured under Change Management of AppViewX Settings.

Compatible Software Versions

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

- AppViewX – Free AppViewX version and version 12.1.0 and version 12.2.0
- ServiceNow – Geneva version and Eureka version

- 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:

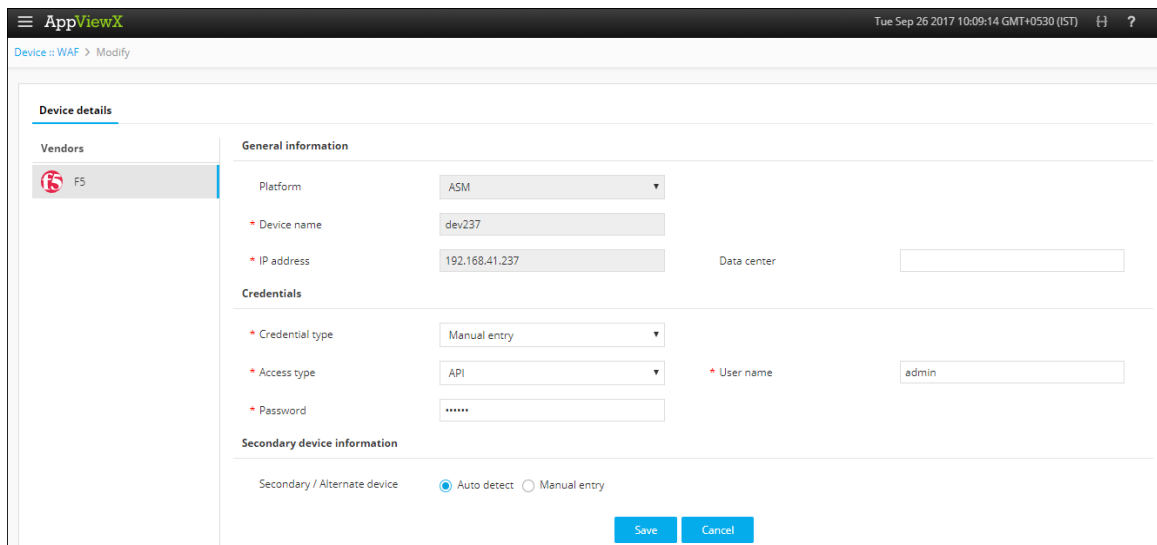
`https://hostname:portnumber.`

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 a Web Application Firewall (WAF): 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 **WAF** tab.
5. On the *WAF inventory* page that opens, click the  (**Add**) button in the Command bar.



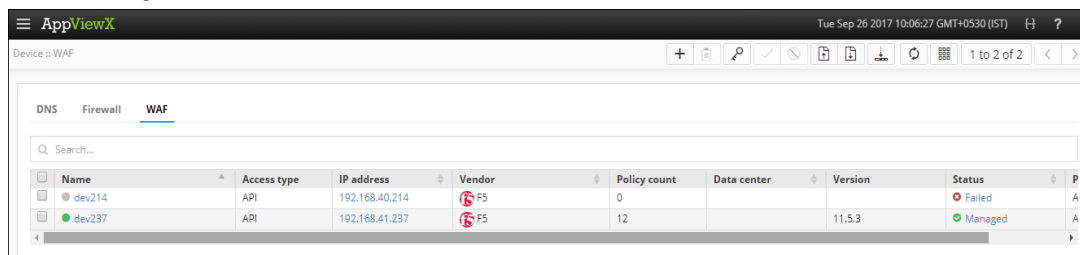
The screenshot shows the AppViewX web interface. The top bar displays 'AppViewX' and the date/time 'Tue Sep 26 2017 10:09:14 GMT+0530 (IST)'. The breadcrumb trail is 'Device > WAF > Modify'. The 'Device details' form is displayed with the 'Vendors' sidebar on the left, where 'F5' is selected. The form contains the following sections and fields:

- General information:**
 - Platform: ASM (dropdown)
 - Device name: dev237 (text field)
 - IP address: 192.168.41.237 (text field)
 - Data center: (empty text field)
- Credentials:**
 - Credential type: Manual entry (dropdown)
 - Access type: API (dropdown)
 - Password: (masked text field)
 - User name: admin (text field)
- Secondary device information:**
 - Secondary / Alternate device: ☒ Auto detect ☐ Manual entry

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

6. In the left-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 to want to provide the credentials:
 - o Select **Manual entry**, if you want to manually enter the credential details (user name and the associated password) every time when the device is accessed.
Also, Select the **Access type** as **API** to help AppViewX to establish a communication and to fetch the configuration once the device is in manage state.
 - o 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.
You must select the credential name from the dropdown list and the **user name** and **password** fields will be auto-filled with the values provided while creating a 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:
 - o Select **Auto detect**, if you want AppViewX to automatically detect and retrieve the configuration of secondary/alternate device, then click **Save** to add the device to AppViewX.
 - o 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**. The secondary device will be displayed in the collection grid.
Note: You can add more than one secondary devices. **Update/Delete** buttons will be enabled only when you try to modify the secondary device that are added.
- h. Click **Save** to add the new WAF device. The device will be displayed in the collection grid under WAF tab.





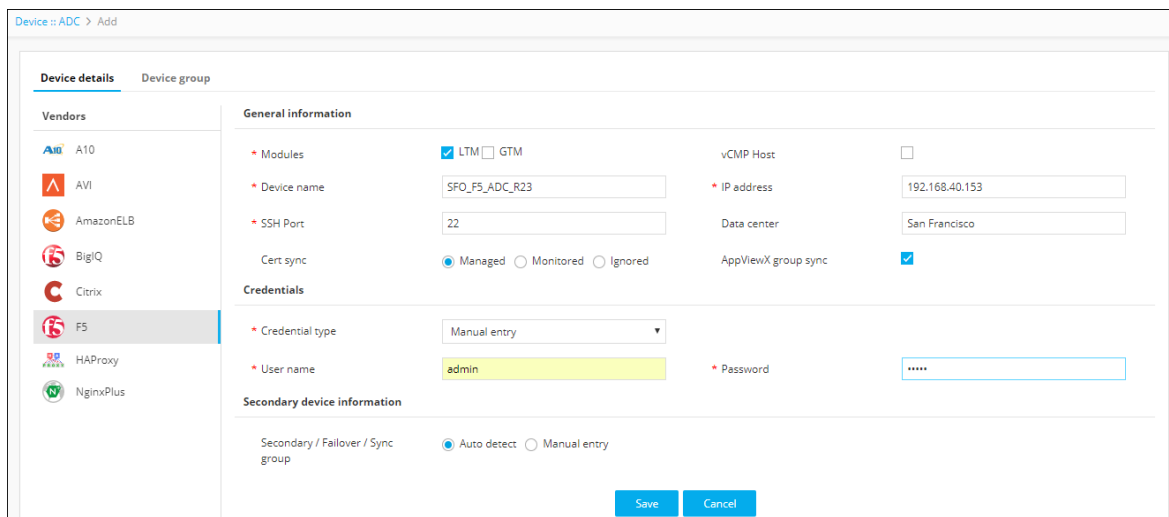
Name	Access type	IP address	Vendor	Policy count	Data center	Version	Status	P
dev214	API	192.168.40.214	F5	0		11.5.3	Failed	A
dev237	API	192.168.41.237	F5	12			Managed	A

The device will display one of the following statuses:

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

Add an ADC Device: 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  (**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 'Add' screen for an ADC device. The breadcrumb is 'Device > ADC > Add'. The left sidebar shows a list of vendors: A10, AVI, AmazonELB, BigIQ, Citrix, **F5** (selected), HAProxy, and NginxPlus. The main area is titled 'Device details' and 'Device group'. It contains several sections: 'General information' with fields for Modules (LTM selected, GTM unselected), Device name (SFO_F5_ADC_R23), SSH Port (22), vCMP Host (checkbox), IP address (192.168.40.153), Data center (San Francisco), and Cert sync (Managed selected, Monitored and Ignored unselected). 'AppViewX group sync' is checked. 'Credentials' section has Credential type (Manual entry), User name (admin), and Password (masked). 'Secondary device information' has a radio button for 'Auto detect' (selected) and 'Manual entry' (unselected). At the bottom right are 'Save' and 'Cancel' buttons.

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 drop-down 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 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.

Register an ITSM Device: ServiceNow

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Settings**.
2. On the *Settings* page that opens, click **Change Management** in the column on the left.
3. Click the **ServiceNow** plug-in.
4. On the *Vendor configuration* screen that opens, enter a valid web URL
5. (Optional) Enter a **Description** of the vendor to help users identify it.
6. Enter the ServiceNow **username** and **password** credentials in the respective fields.
7. Click **Update** to save the changes made in the system.

Settings :: Change Management > Vendor configuration

Authentication

SSH

Certificate

Provisioning

Change Management

ADC

Backup & Restore

Log forwarding

License

System

AppViewX

Information

Name: Change

Description:

URL: https://ven01189.service-now.com

Upload image:

Username: admin

Password:

General settings

Active Provisioning Instance: ☒

Device / CI validation: ☐

Timezone: GMT

Implementation mode: Stop

Enable polling: ☐

Polling interval (mins): 5

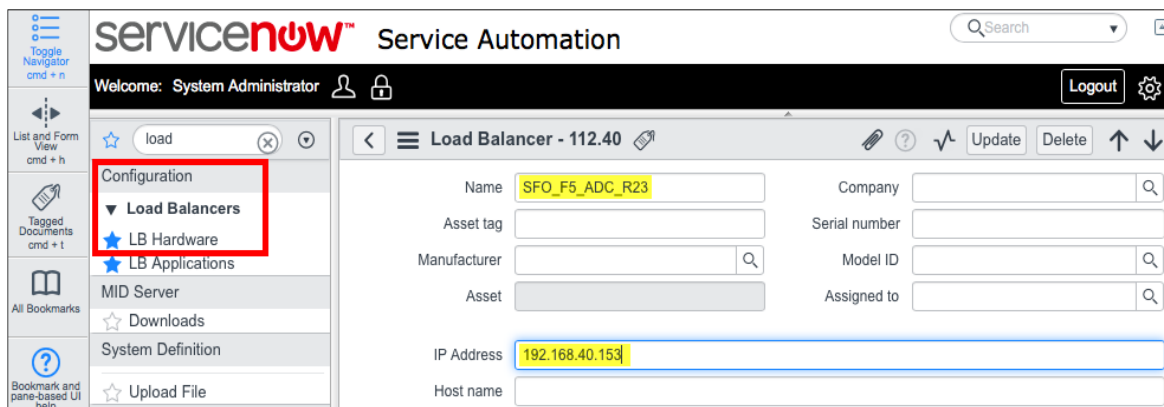
Approve mode: Stop

Log / Configuration settings

Select configuration type: Pre validation, Post validation

Consolidated logs: ☒

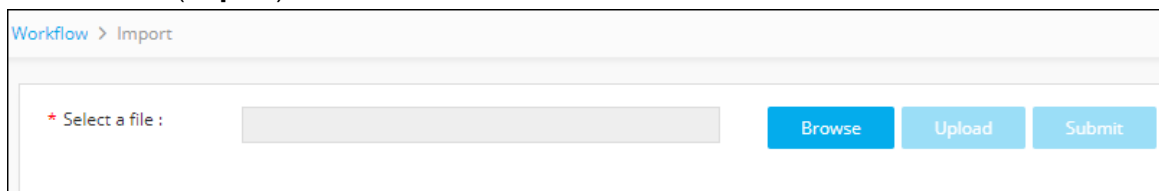
8. (Optional) The F5 LTM device you are configuring should be present in the ServiceNow LB Hardware inventory. You can check this by opening ServiceNow and clicking to open the Load Balancers > LB Hardware section as shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.



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. To import a workflow, complete the following sub-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.

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 Migration 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 Migration 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 Migration workflow from the Card view by clicking the  (**Disable**) button.







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

ASM Policy Migration workflow

To submit the ASM Policy Migration 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 ASM Policy Migration workflow.
4. On the *Form Builder* screen that opens, click the **Get Source WAF Device** button to retrieve the list of F5 LTM devices.

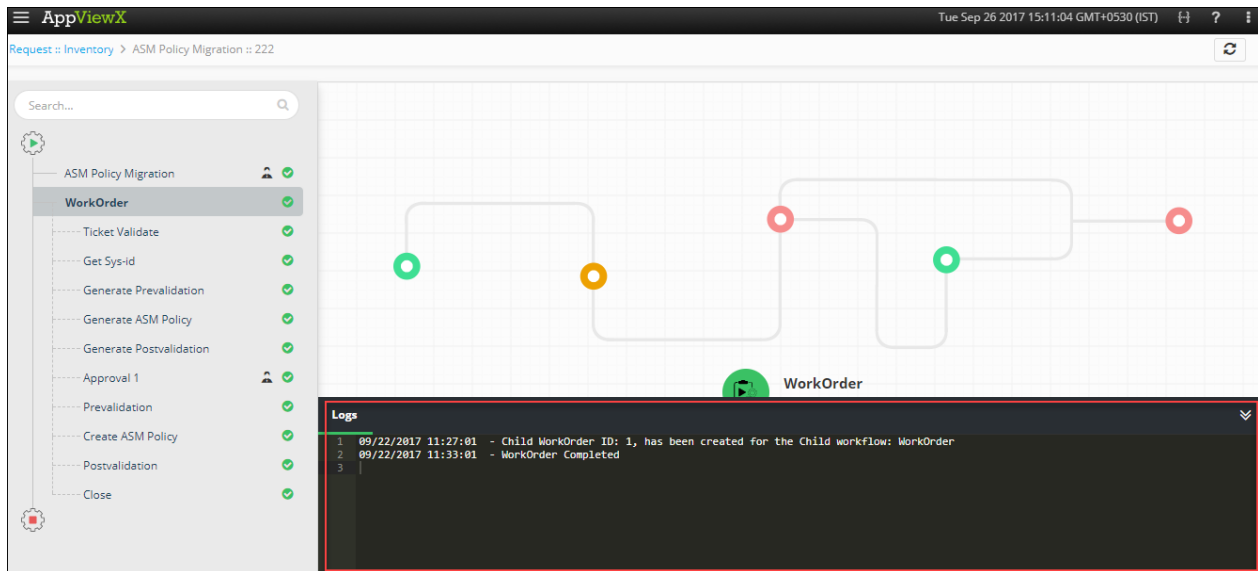
5. From the **Source Device** dropdown list, select the device from which you want to migrate the policy.
6. Click the **Get ASM Policy** button to retrieve the list of ASM policies available in the source device.
7. From the **Policy list** dropdown filed, select the policy you want to migrate to the target device
8. In the **Field Name** field, click the  (**Retrieve field values**) button to fetch the file name (from the database) in which the policy resides.
9. Click **Get Target WAF Device List** to retrieve the list F5 target devices.
10. From the **Target Device** dropdown list, select the device to which the ASM policy has to be migrated.
11. In the **Target Policy Name** field, enter the name for the policy to be created on the target device.
12. Click the **Get Target Device Virtual Servers** button to retrieve the virtual servers present in the destination device.
13. From the **Virtual Server** dropdown list, select the virtual server in order to associate a policy.
14. Depending on whether or not you want to integrate the ITSM tool – ServiceNow, select the **Yes** or **No** radio button. To integrate the ITSM tool, enter the following details:
 - a. In the **Time Zone** dropdown list, click the  (**Retrieve field values**) button to retrieve the time zone. Select the time zone for the F5 LTM device that you configure.
 - b. Schedule the service window time and date using the **Start Date** and **End Date** fields. Click the  (**Calendar**) button to select the start and end date respectively. The configuration changes will be implemented during this service window.
 - c. In the **Create ServiceNow Ticket** field, click the  (**Retrieve field values**) button to retrieve the ticket number.
15. Click **Submit**.

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

WorkOrder flow

Following are the workorder tasks of ASM Policy Migration 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. **Ticket Validate** — to validate the ticket, you will have to log in to the ITSM tool- ServiceNow and manually approve the ticket.

2. **Get Sys ID** — the Sys-ID for the ASM Policy Migration workflow is generated to track the ServiceNow request.
3. **Generate Prevalidation** — the pre-validation commands are generated in order to initiate the pre-validation process.
4. **Generate ASM Policy** — the configuration commands are generated to migrate the ASM policy from the source device to the target device.
5. **Generate Postvalidation** — the post validation commands are generated in order to initiate the post-validation process.
6. **Implementation Approval** — 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.

Prevalidation	Implementation <pre> 1 <device>99.11</device> 2 tmsb 3 create asm policy testasm12345 active 4 load asm policy testasm12345 overwrite file /var/tmp/2017-09-22_11:25:44_exported_policy_as.app 5 create ltm policy Drafts/testasm12345 controls add { asm } requires add { http } rules add { d 6 publish ltm policy Drafts/testasm12345 7 modify ltm virtual vs_great_80 policies add { testasm12345 } profiles add { websecurity } 8 save sys config 9 quit 10 </pre>
Postvalidation	
Implementation	
Comments <input type="text"/>	
<input type="button" value="Implement"/> <input type="button" value="Reject"/> <input type="button" value="Cancel"/>	

7. **Prevalidation** — check the following:
 - A list of ASM policies available in the source and target device.
 - The ASM policy that you want to migrate from a source device is not available on the target device.
 - The performance metrics such as CPU and memory utilization on the destination device are validated.
8. **Create ASM Policy** — An ASM policy is migrated from the source device to the target device with a new policy name. It is then associated to a virtual server selected on the target device.
The ASM Policy Migration will be implemented during the service window you selected while integrating the ITSM tool-ServiceNow.
Note: The request fails when the ServiceNow ticket is not approved before the service window starts.
9. **Post-Validation** — checks if the ASM policy you selected from the source device are migrated successfully to the destination or target device.
10. **Close** — after the policy migration is successful, the status of the ServiceNow ticket will be automatically updated to *Closed Complete*.

ServiceNow Service Automation

System Administrator CHG0035807

Filter navigator

Self-Service

APS Templates

Device

form1

Guided Setup

PagerDuty

Service Desk

Incident

Problem

Exact search match. Click here to see full search results.

Number: CHG0035807

Requested by: System Administrator

Category: Hardware

Configuration item:

Priority: Low

Impact: 1 - High

Description: ASM Policy Migration

Approval: Approved

Type: Comprehensive

State: Closed Complete

Conflict status: Not Run

Conflict last run:

Assignment group:

Assigned to:

Work notes:

Planning

Change plan: tmsh
load asm policy testasm12345 overwrite file /var/tmp/2017-09-22_11:25:44_exported_policy_as.appviewx.com.xml
load asm policy testasm12345 active
quit


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.

AppViewX

Tue Sep 26 2017 15:05:53 GMT+0530 (IST)


Request > Inventory

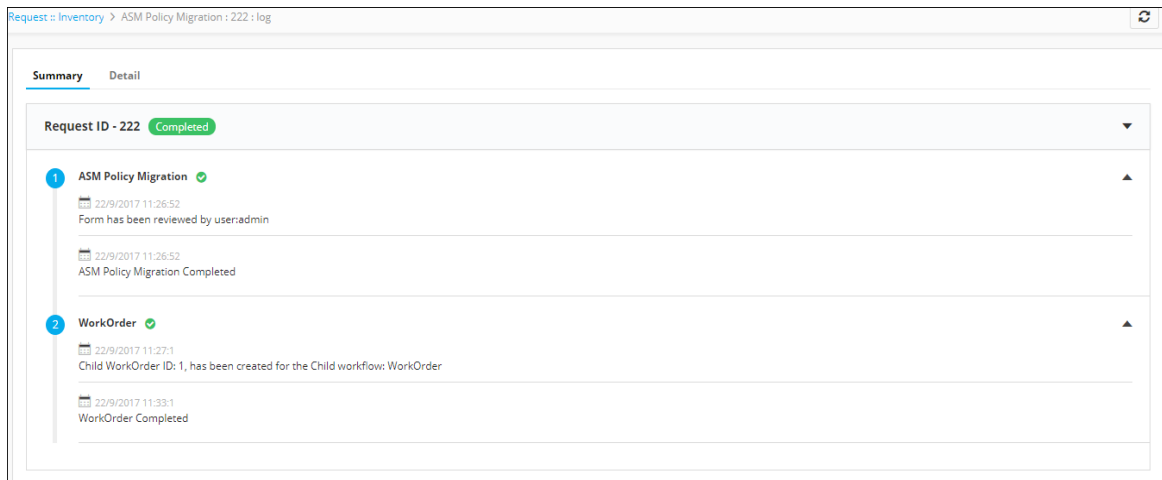
1 to 100 of 229

My catalog **Request Inventory** Scheduled workflows

Search...



Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
229	Modify Virtual Server	admin	26/09/2017 03:00 PM	26/09/2017 03:00 PM	In Progress	View
228	ASM Policy Creation	admin	26/09/2017 03:00 PM	26/09/2017 03:00 PM	In Progress	View
227	ASM Policy Creation	admin	26/09/2017 02:58 PM	26/09/2017 02:58 PM	In Progress	View
226	ASM Policy Creation	admin	26/09/2017 02:53 PM	26/09/2017 02:53 PM	In Progress	View
225	ASM Policy Creation	admin	26/09/2017 02:47 PM	26/09/2017 02:47 PM	In Progress	View
224	ASM Policy Creation	admin	26/09/2017 02:41 PM	26/09/2017 02:41 PM	In Progress	View
223	ZTP of BIG-IP VE	admin	22/09/2017 11:56 AM	22/09/2017 11:56 AM	Completed	View
222	ASM Policy Migration	admin	22/09/2017 11:26 AM	22/09/2017 11:26 AM	Completed	View

4. Click the **Request ID** created for ASM Policy Migration 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: by whom and when the Request was created, Last updated time, Status and the 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.






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 ASM Policy Migration workflow.
4. On the ASM Policy Migration 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 here.
5. Click **Save**.

Scheduled workflows

Displays all workflows that have been scheduled. 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 **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 ASM Policy Migration 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.

I cannot retrieve the Virtual Server details

The F5 ASM devices should be added under both WAF and ADC sections in the AppViewX inventory. For more details on how to add an ADC/WAF device, refer to the Add an [Add](#) an ADC

Device: F5 LTM/ [Add](#) a Web Application Firewall (WAF): F5 LTM device section of this guide.

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

You must add an ASM device in the AppViewX inventory with the admin user privileges. For more details on how to add an ADC/WAF device, refer to the Add an [Add](#) an ADC Device: F5 LTM/ [Add](#) a Web Application Firewall (WAF): F5 LTM device section of this guide.