AppViewX

ASM Policy Migration Workflow Guide

Trademarks

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: 1.3

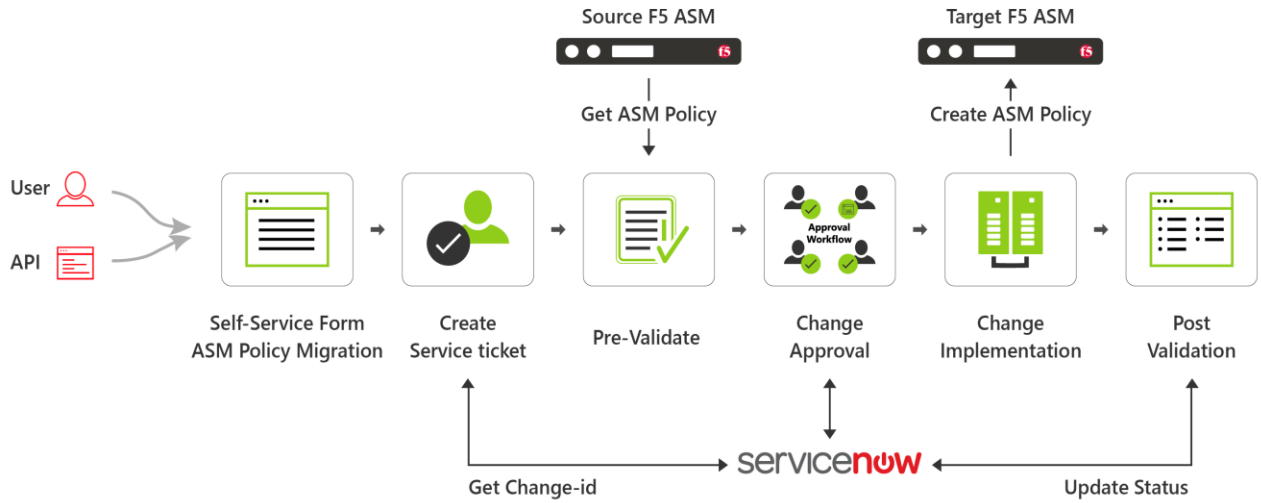
Last updated on: December 15, 2017

Contents

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 with a virtual server present in the destination device. Also, you have the option to integrate the workflow with an ITSM tool called 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 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.
- The F5 ASM devices have been added under both the WAF and ADC sections in the AppViewX inventory.
- Each ADC device is a managed entity in AppViewX.
- You have administrator permissions to add a device to the AppViewX inventory.
- An ITSM tool (ServiceNow) has been configured under the Change Management section of the AppViewX Settings module.

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
- 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

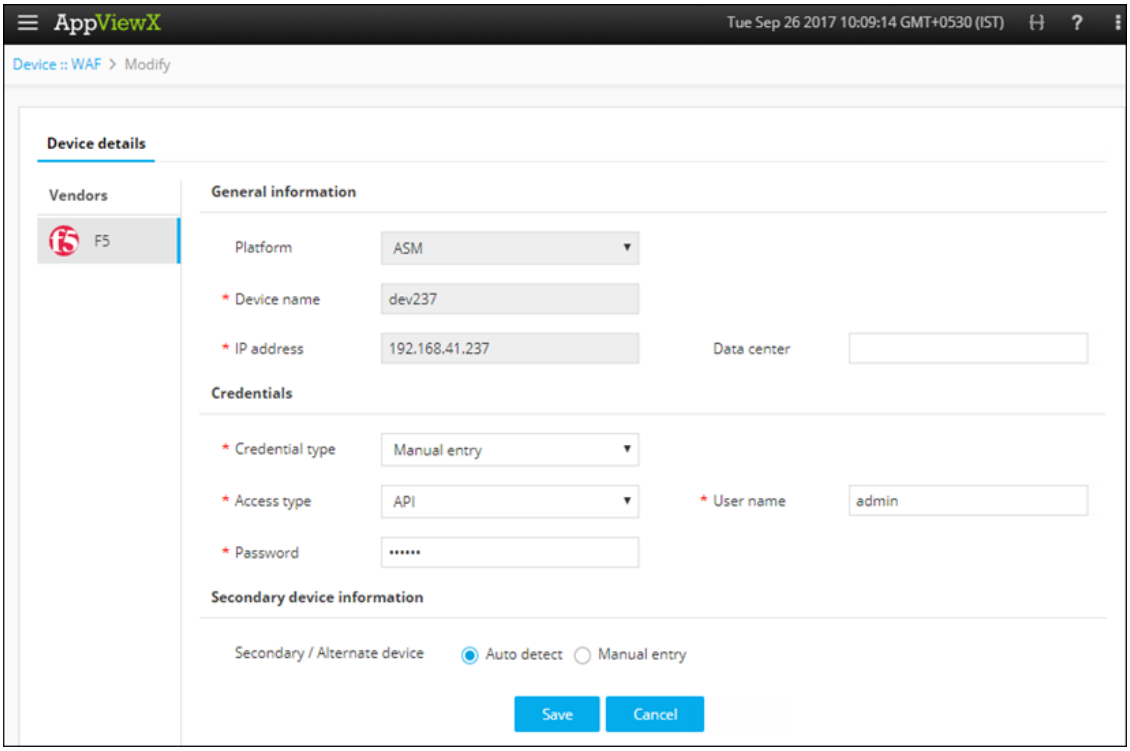
Log in to the AppViewX web interface. The standard format for a login URL is: `https://hostname:portnumber`.

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.
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.



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.

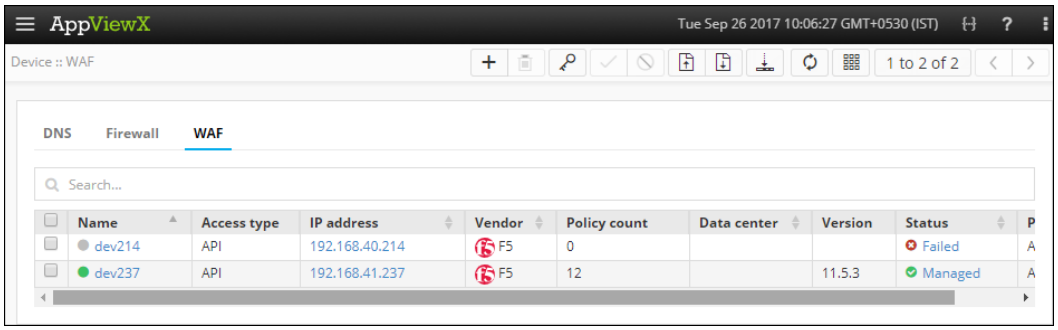
          When you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.

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.

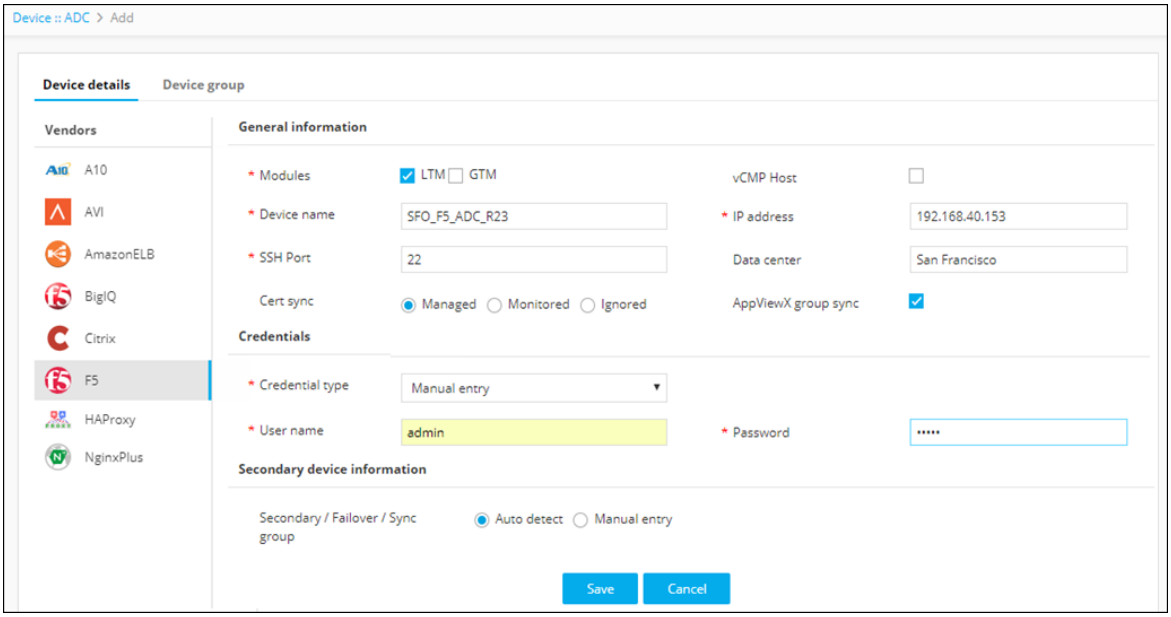


The device will display one of the following statuses:

- **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.

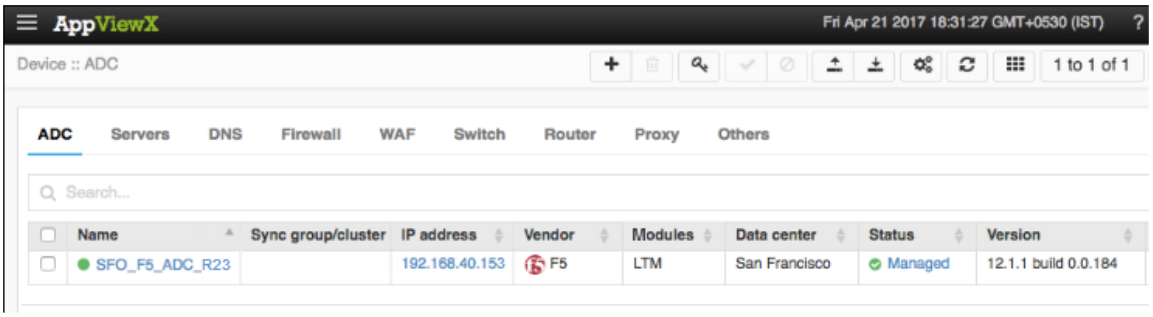
Add an ADC Device: F5 LTM

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.



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. Create 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. 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**.
12. (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.
13. Select a **Credential type** from the dropdown menu.
14. 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.
15. Select **Auto detect** to automatically detect and add secondary or failover devices or sync groups to the ADC device inventory.
16. Click **Save** to save the new ADC device in the table on the ADC tab.

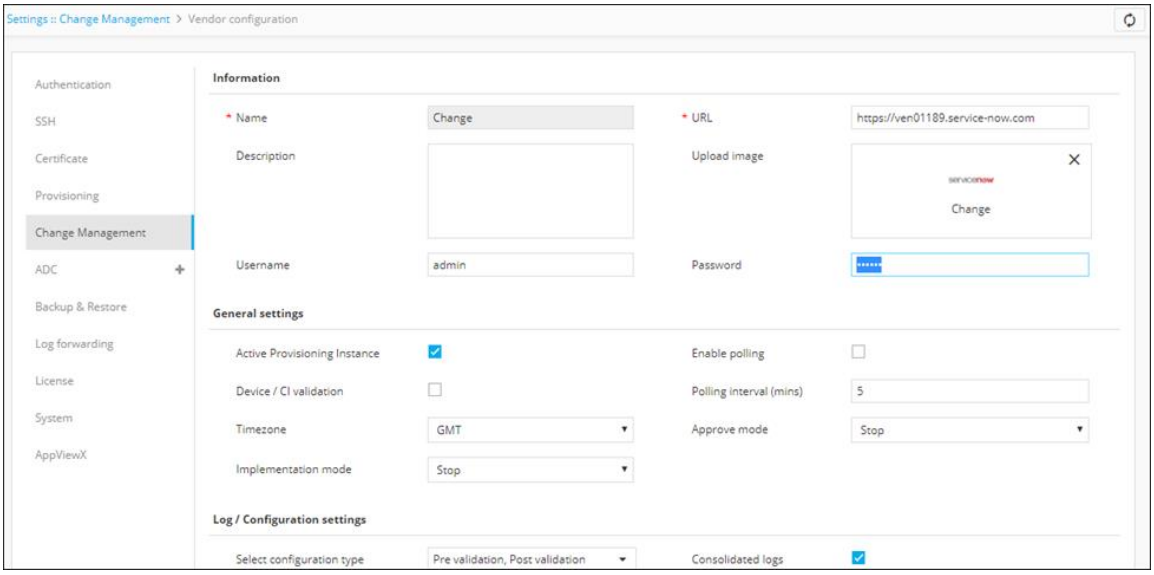


The device will display one of the following statuses:

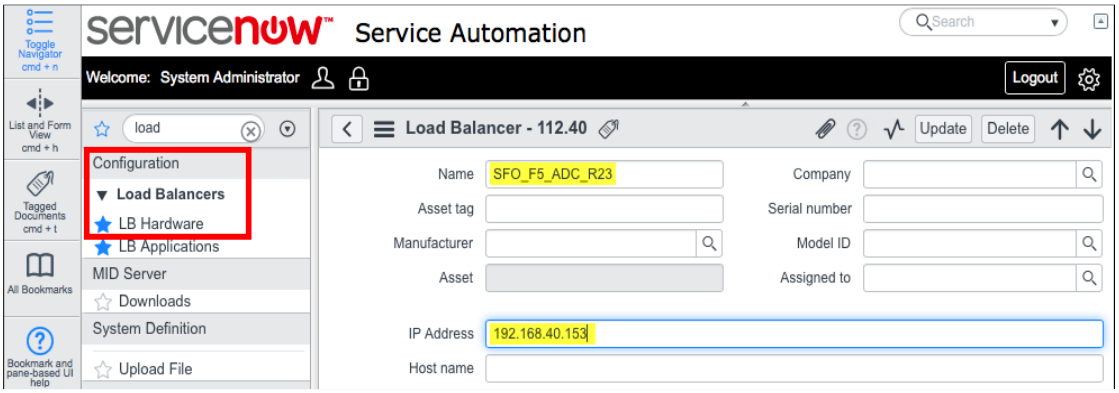
- **In Progress** – Device configuration fetch is in progress.
- **Managed** - Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device due to invalid login credentials.
- **Failed**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

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* screen 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.



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 shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.

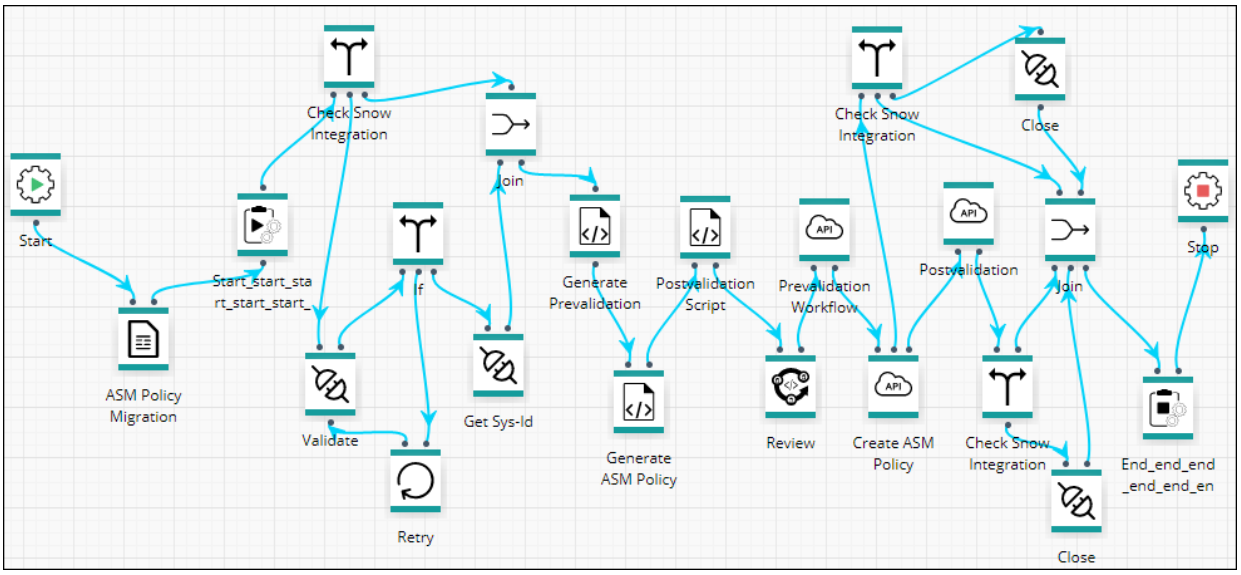


Import Visual Workflows

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* screen, select the check box beside the unzipped workflow file.
    d. Click **Submit** to deploy the workflow into your AppViewX environment.

The ASM Policy Migration 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* screen, select the check boxes beside each of the helper scripts.
    e. Click **Submit** to deploy them into your AppViewX environment.

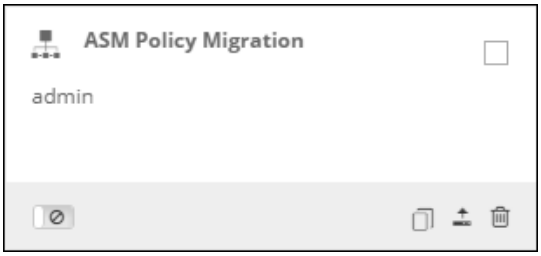
Enable a Workflow

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**.

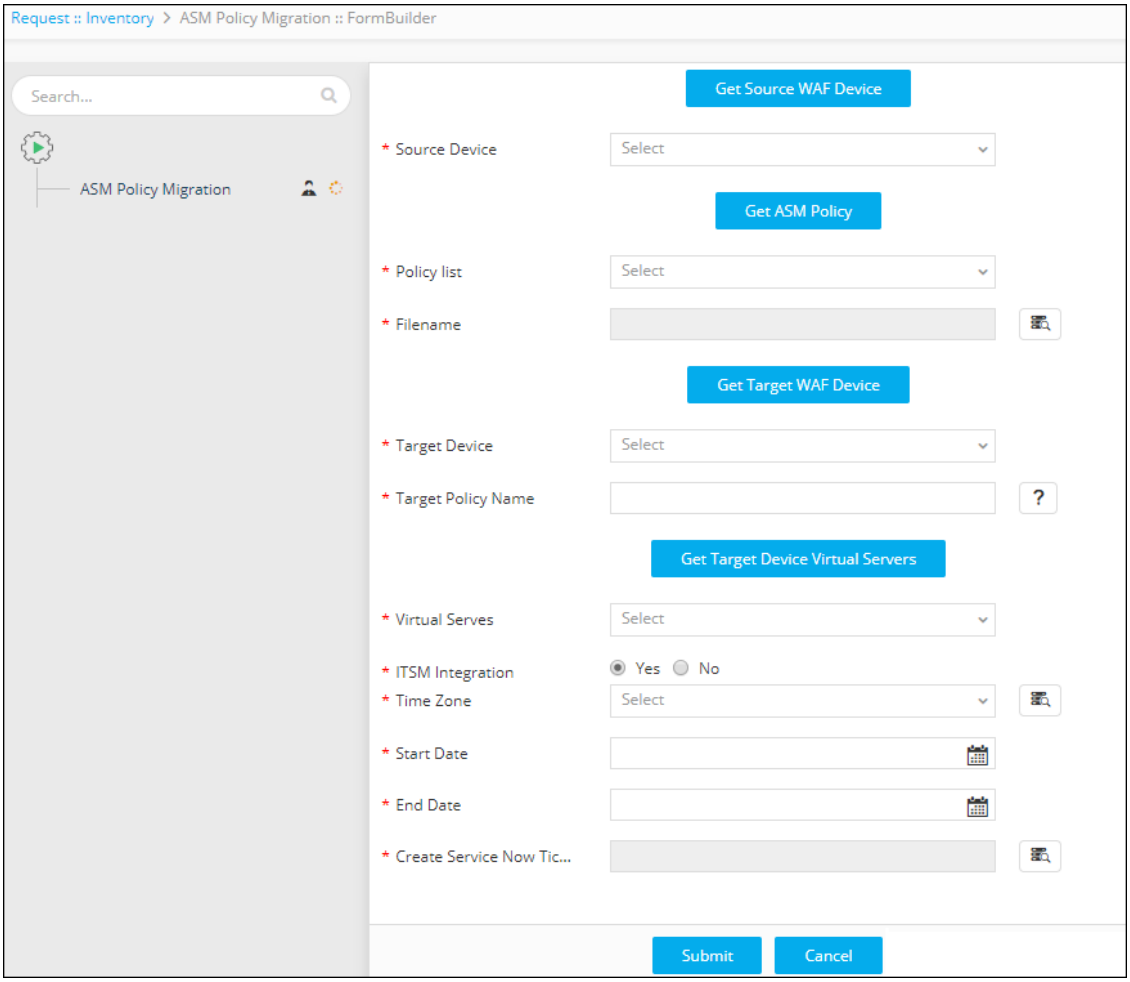
ASM Policy Migration Workflow

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 the ASM Policy Migration workflow.

   The *Form Builder* screen opens.



4. 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 field, 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.

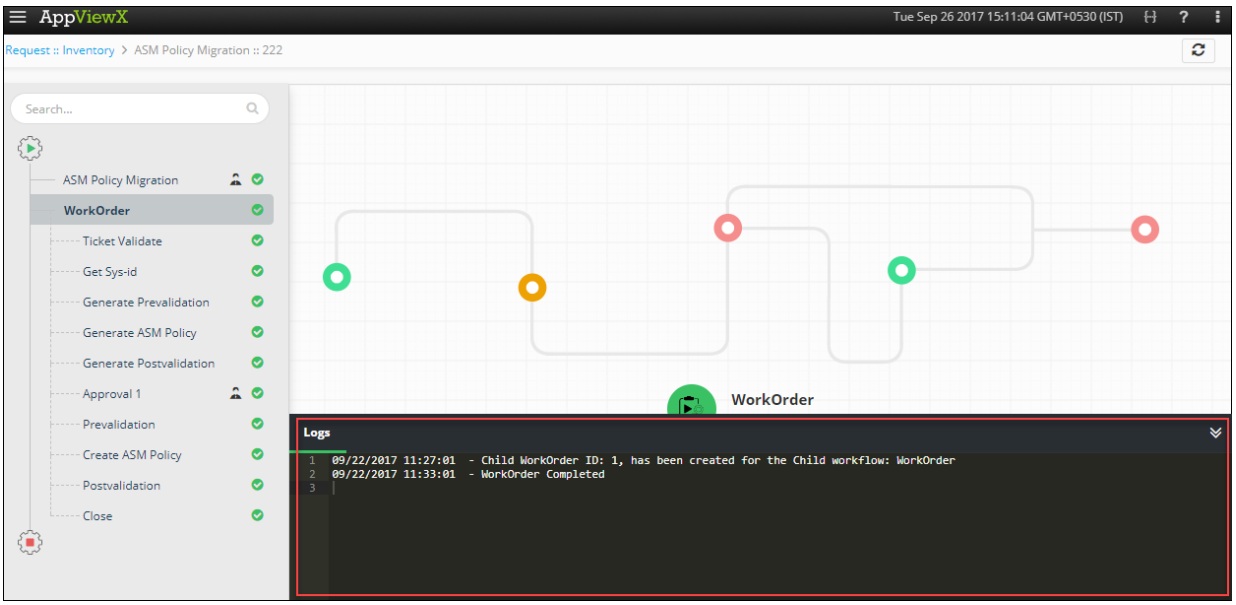
14. Depending on whether or not you want to integrate the ITSM tool – ServiceNow, select the **Yes** or **No** radio button. To integrate the ITSM tool, enter the following details:
    a. In the **Time Zone** dropdown list, click the (**Retrieve field values**) button to retrieve the time zone. Select the time zone for the F5 LTM device that you are configuring.
    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. 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 ServiceNow ticket number.
15. Click **Submit**.

    A new **Request ID** is created. To view all requests, refer to the Request Inventory section of this guide.

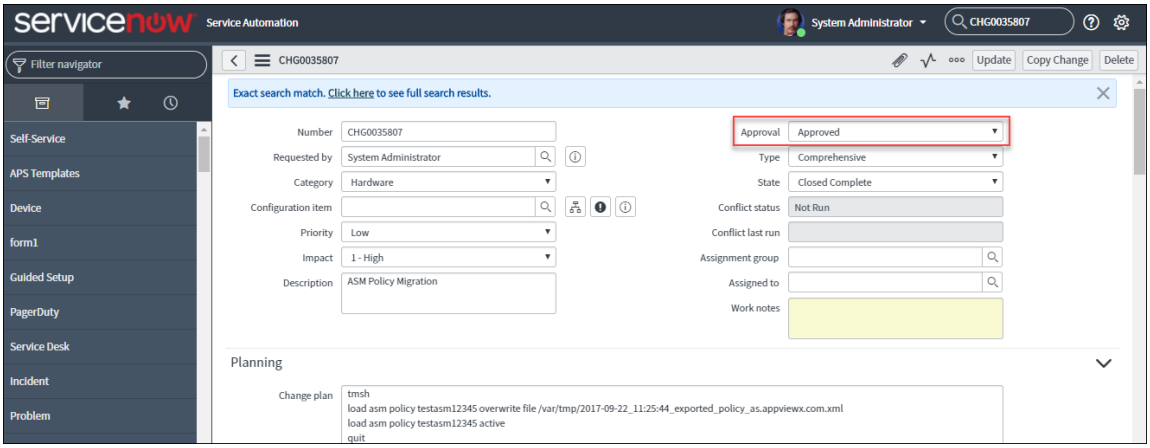
WorkOrder Flow

The following are the workorder tasks for the ASM Policy Migration workflow.

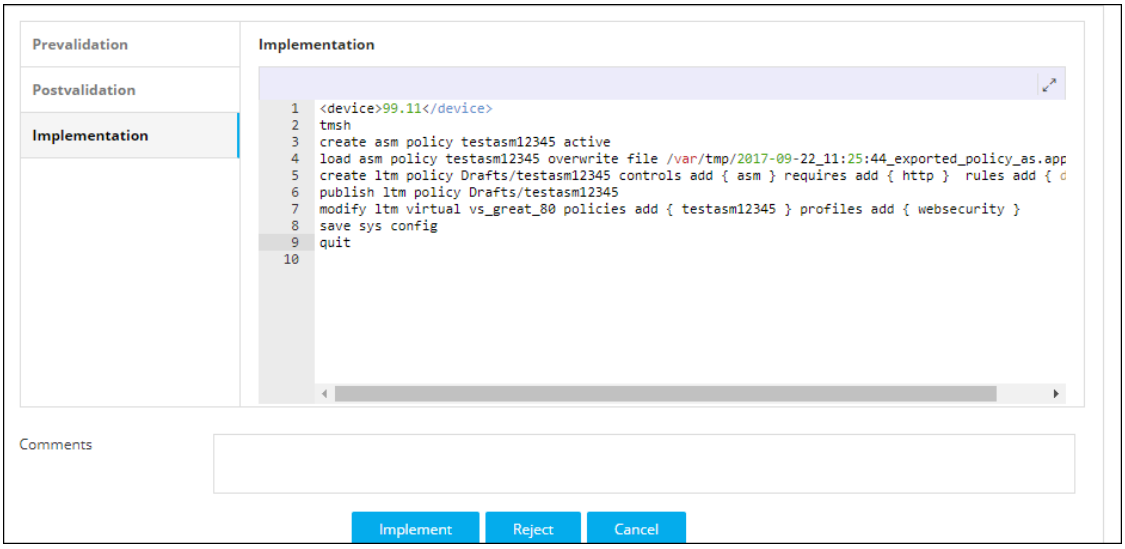
Note: You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.



1. **Ticket Validate** – To validate the ticket, 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** – Pre-validation commands are generated to initiate the pre-validation process.
4. **Generate ASM Policy** – Configuration commands are generated to migrate the ASM policy from the source device to the target device.
5. **Generate Postvalidation** – Post validation commands are generated 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 approval and implementation permissions. After you submit the request form, the configuration changes are reviewed and approved at AppViewX. The configuration changes are implemented on the device only after approval is received.

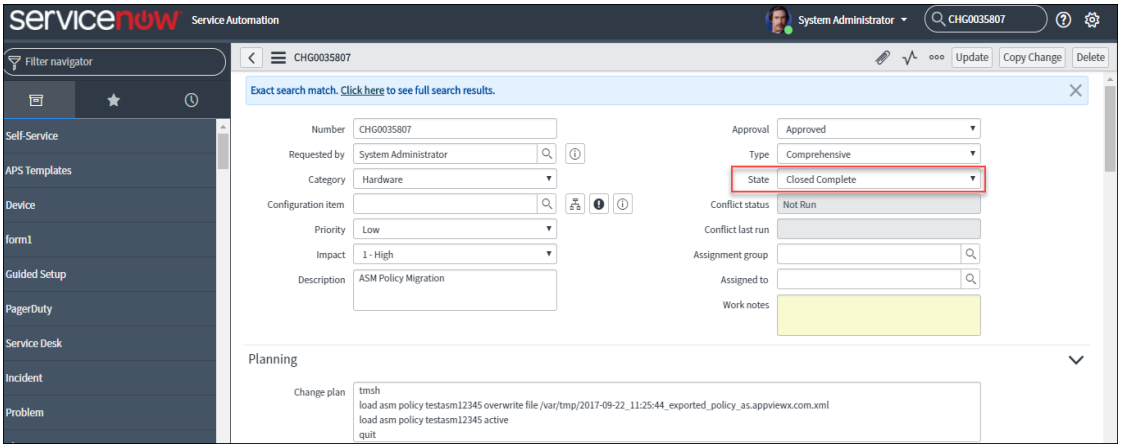


7. **Prevalidation** – Check the following:
    - A list of ASM policies is available in the source and target device.
    - The ASM policy that you want to migrate from a source device is not available on the target device.
    - The performance metrics, such as CPU and memory utilization on the destination device, have been 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 with 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 will fail if 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 was migrated successfully to the destination or target device.
10. **Close** – After successful migration of the policy, the status of the ServiceNow ticket updates automatically to *Closed Complete*.



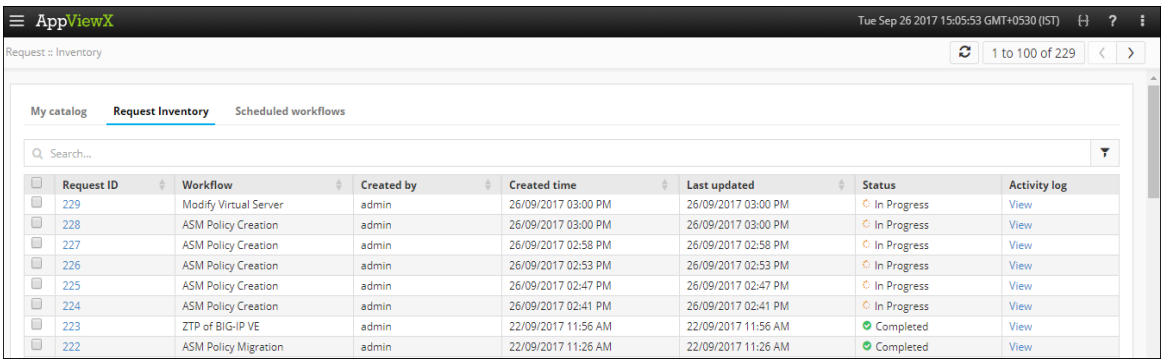
Request Inventory

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

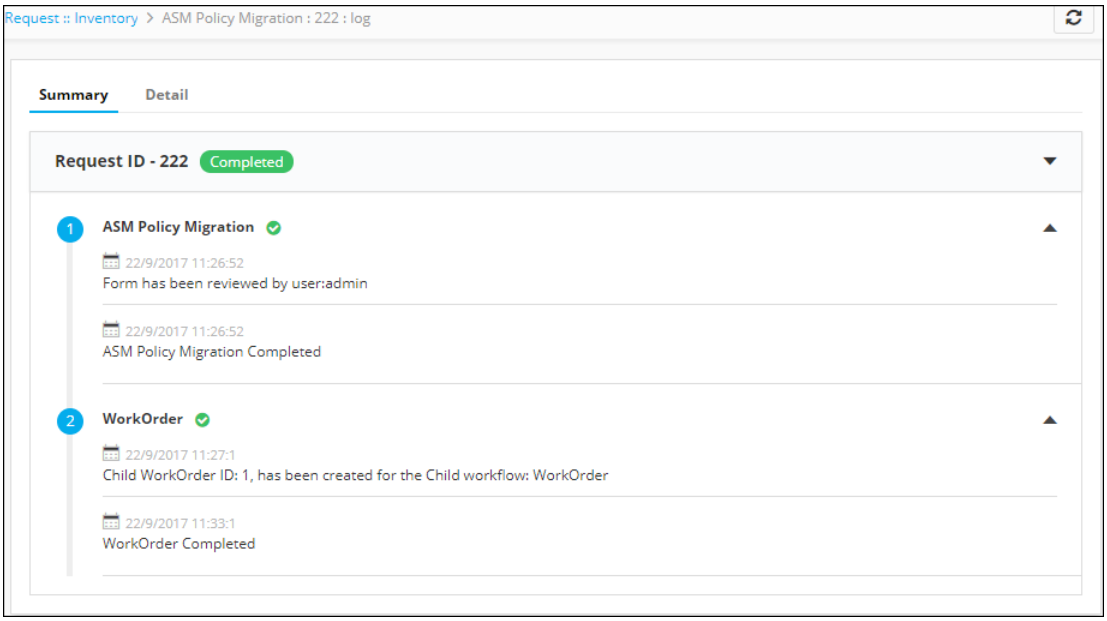
1. Click the  (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   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.



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 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.



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 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.
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 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 or WAF device, refer to the Add an ADC Device: F5 LTM and Add a Web Application Firewall (WAF): F5 LTM sections of this guide.

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

You must have Admin user privileges in order to add an ASM device to the AppViewX inventory. For more details on how to add an ADC or WAF device, refer to the Add an ADC Device: F5 LTM and Add a Web Application Firewall (WAF): F5 LTM sections of this guide.