AppViewX

Create Wide IP with SNAT and Traffic Group 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: 1.0

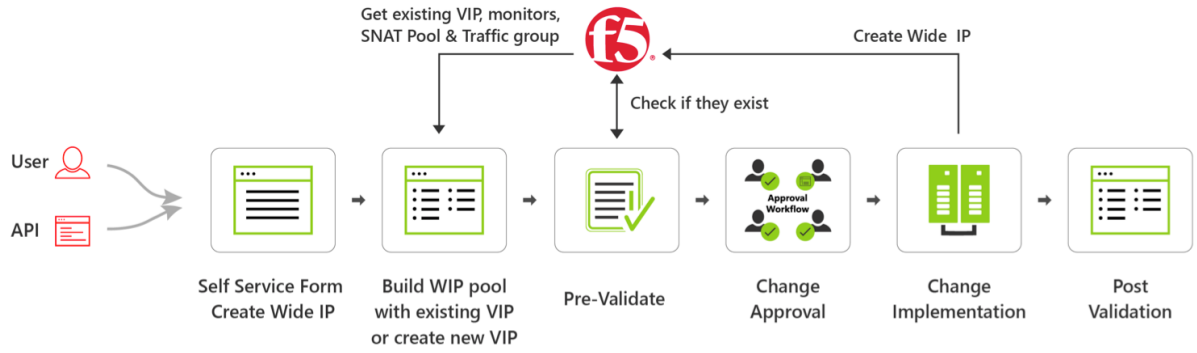
Last updated on: December 18, 2017

Contents

Description

The “Create Wide IP with SNAT and Traffic Group” workflow is used to create multiple virtual servers (VIP) under a single Wide IP. In this workflow, either a virtual server (that are classified into two categories such as an existing virtual server and new virtual server) or a generic host (an end server) is added as a new pool member to the Wide IP. You can also create a new virtual server pool with or without associating it to the existing monitor, SNAT pool, and traffic group.

The flow diagram of Create Wide IP with SNAT and Traffic Group 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 temple has been tested and validated on the following software versions:

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

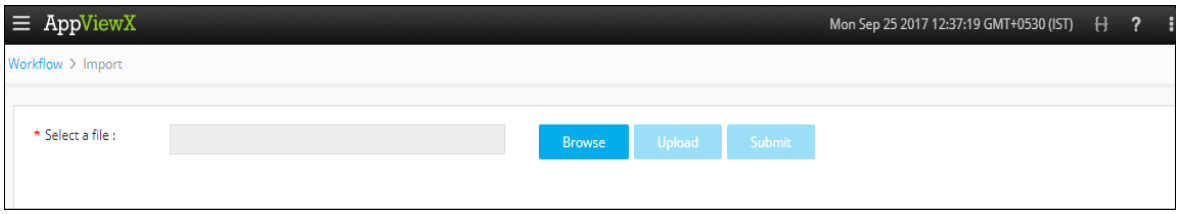
The hostname and port number are configured during deployment, with the default port number set to `5004` and the default web credentials set to `admin`/`AppViewX@123`.

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

Import Visual Workflows

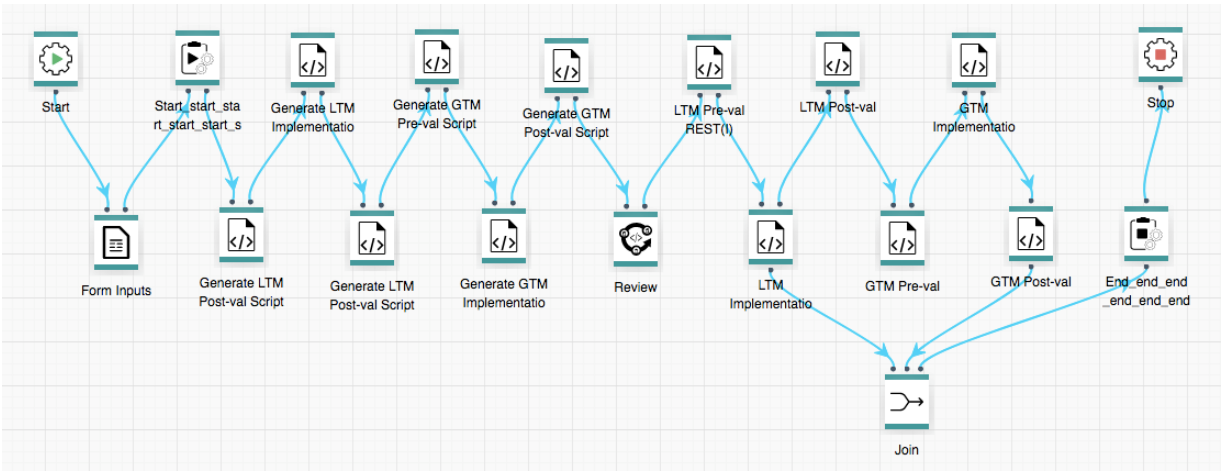
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

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.

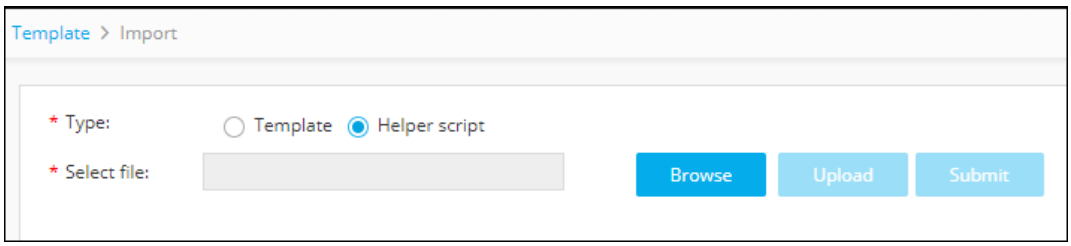
The Create Wide IP with SNAT and Traffic Group workflow is shown in the image below:



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.

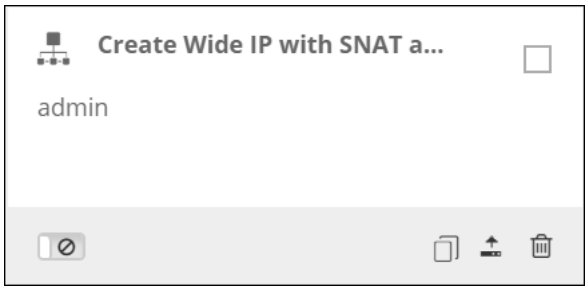
Enable a Workflow

To enable the Create Wide IP with SNAT and Traffic Group 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 Create Wide IP with SNAT and Traffic Group workflow to enable. If the workflow is already selected, a (**Deselect**) button appears.
4. Click the (Enable) button in the Command bar.

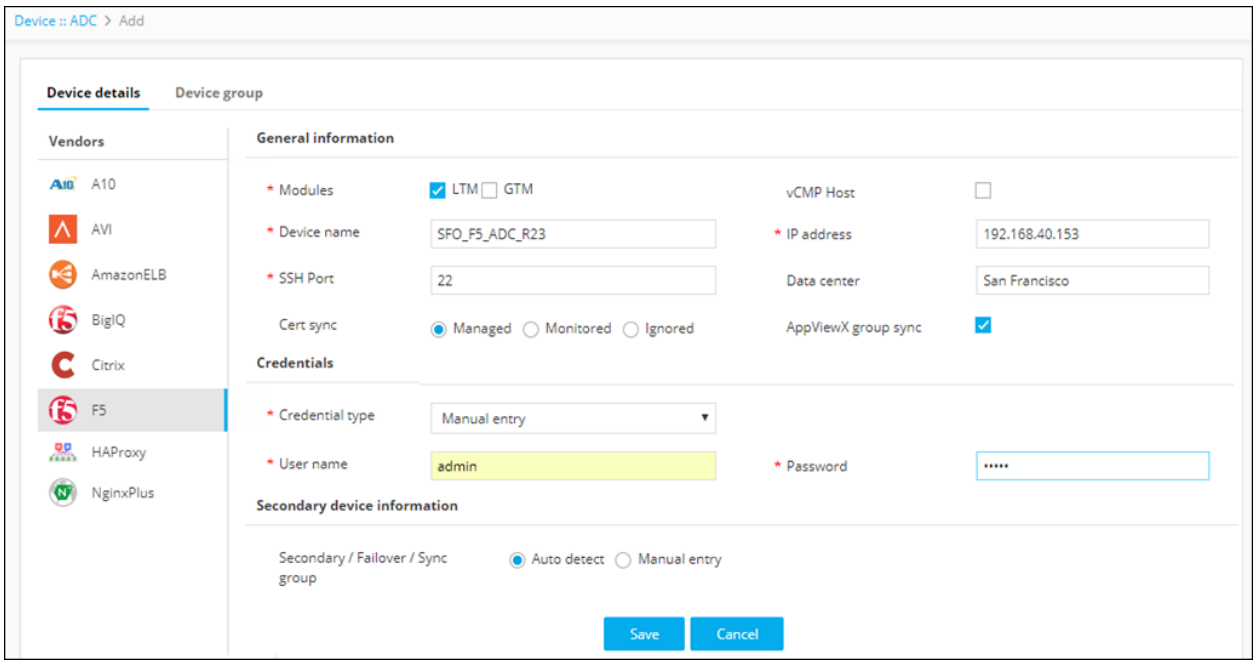
   Note: You can also enable the Create Wide IP with SNAT and Traffic Group workflow from the Card view by clicking the (**Disable**) button.



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

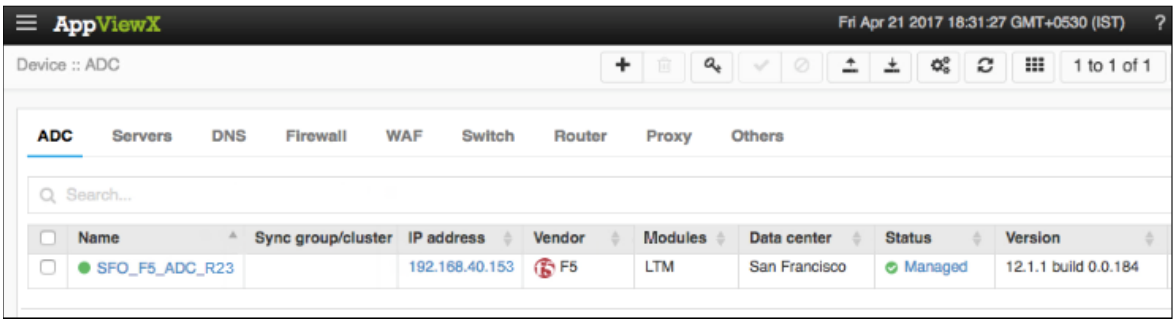
Add an ADC Device: F5

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.



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.

Create Wide IP with SNAT and Traffic Group Workflow

To submit the Create Wide IP with SNAT and Traffic Group 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 Create Wide IP with SNAT and Traffic Group, the respective Form Builder screen opens.
4. On, in the **Wide IP Device** field, click the  (**Retrieve field values**) button to retrieve the GTM devices present in the AppViewX inventory. Select the Wide IP device from the drop-down list.
5. In the **WIP Name** field, enter the name for the Wide IP.
6. (Optional) In the **Alias name** field, enter the alias name for the Wide IP.
7. In the **Wide IP Pool Name** field, click the  (**Retrieve field values**) button to retrieve the relevant pool name (field values) present in the AppViewX inventory.
8. From the **Preferred**, **Alternate**, and **Fallback** drop-down fields, select one of the load balancing method for the Wide IP pool: **global-availability** or **round-robin**.
9. From the **Wide IP Pool Member Type** drop-down list, select one of the following pool member for the Wide IP:
   - **Generic host**
   - **VIP**
10. If Generic host is selected as the Wide IP pool member, enter the following details:
    a. In the **Wide IP Data Center** field, click the  (**Retrieve field values**) button to retrieve the data centers of the GTM devices. Select the data center from the drop-down list.
    b. Enter the IP address and port details of the Generic Host in the respective fields.
11. If VIP is selected as the Wide IP pool member, enter the following details:
    a. In the **Wide IP Data Center** field, click the  (**Retrieve field values**) button to retrieve the data centers of the GTM devices. Select the data center from the drop-down list.
    b. From the **VIP selection** drop-down list, select one of the VIPs: **Use existing virtual** or **Create new virtual**
    c. If **Use existing virtual** option is selected, enter the following details:

i. In the **GTM Server** field, click the  (**Retrieve field values**) button to retrieve the existing GTM server from the selected device. Select the GTM server from the drop-down list.

ii. In the **Select VIP** field, click the  (**Retrieve field values**) button to retrieve the existing virtual server from the selected device. Select the virtual server from the drop-down list.

d. If **Create new virtual** option is selected, enter the following details:

i. In the **LTM Device** field, click the  (**Retrieve field values**) button to retrieve the LTM devices present in the AppViewX inventory. Select an LTM device from the drop-down list.

ii. Enter the name, IP address, port details and description for the virtual server in the respective fields.

iii. Select one of the protocol for the virtual server: **TCP** or **UDP**

iv. Enter the name of the pool member for the virtual server that you want to create.

v. Enter the pool members in the following format in a separate line: IP address, Port number, and so on.

vi. Depending on whether or not you want to use the existing monitors, click the **Yes** or **No** radio button. If you have selected 'Yes', then **Existing monitors field** appears. Click the  (**Retrieve field values**) button to retrieve the existing monitors that are available in the device for selection.

vii. Depending on whether or not you want to use the existing SNAT pool, click the **Yes** or **No** radio button. If you have selected 'Yes', then **Existing SNAT pool** field appears. Click the  (**Retrieve field values**) button to retrieve the existing SNAT pool that are available in the device for selection.

vii. Depending on whether or not you want to use the existing traffic group, click the **Yes** or **No** radio button. If you have selected 'Yes', then **Existing Traffic group** field appears. Click the  (**Retrieve field values**) button to retrieve the existing traffic groups that are available in the device for selection.

12. Click the  (**Add**) button. The Wide IP pool member details will be displayed in the collection grid.

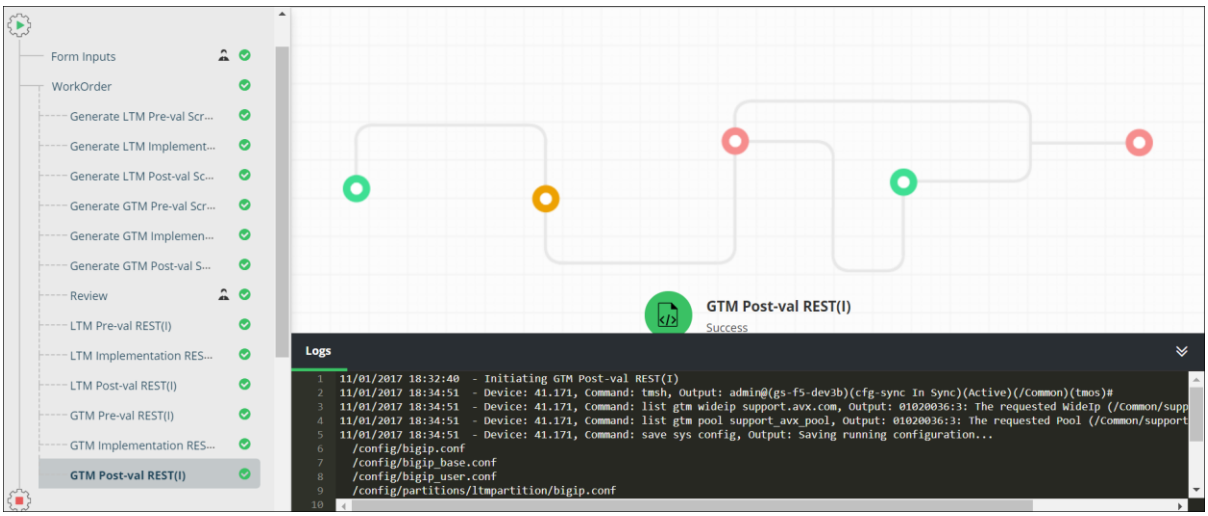
    Note: You also have an option to edit, reset, and delete the details provided.

13. Click **Save draft** to save a draft of the template, which can be submitted later, or click **Submit** to submit the template immediately.

WorkOrder flow

Following are the workorder tasks of Create Wide IP with SNAT and Traffic Group 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 LTM Pre-val Script** — Configuration commands are generated to initiate the LTM pre-validation process.
2. **Generate LTM Implementation Script** — Configuration commands are generated to initiate the LTM implementation process.
3. **Generate LTM Post-val Script** — Configuration commands are generated to initiate the LTM post-validation process.
4. **Generate GTM Pre-val Script** — Configuration commands are generated to initiate the GTM pre-validation process.
5. **Generate GTM Implementation Script** — Configuration commands are generated to initiate the GTM implementation process.
6. **Generate GTM Post-val Script** — Configuration commands are generated to initiate the GTM post-validation process.
7. **Review** — You can review the configuration commands generated in steps 1-6.
8. **LTM Pre-val REST(I)** — LTM pre-validation is initiated using the configured REST API.
9. **LTM Implementation REST(I)** — LTM implementation is initiated using the configured REST API.
10. **LTM Post-val REST(I)** — LTM post-validation is initiated using the configured REST API.
11. **GTM Pre-val REST(I)** — GTM pre-validation is initiated using the configured REST API.
12. **GTM Implementation REST(I)** — GTM implementation is initiated using the configured REST API.
13. **GTM Post-val REST(I)** — LTM post-validation is initiated using the configured REST API.

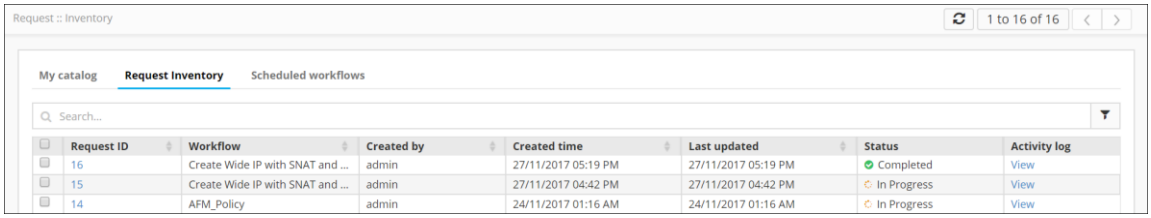
Request Inventory

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

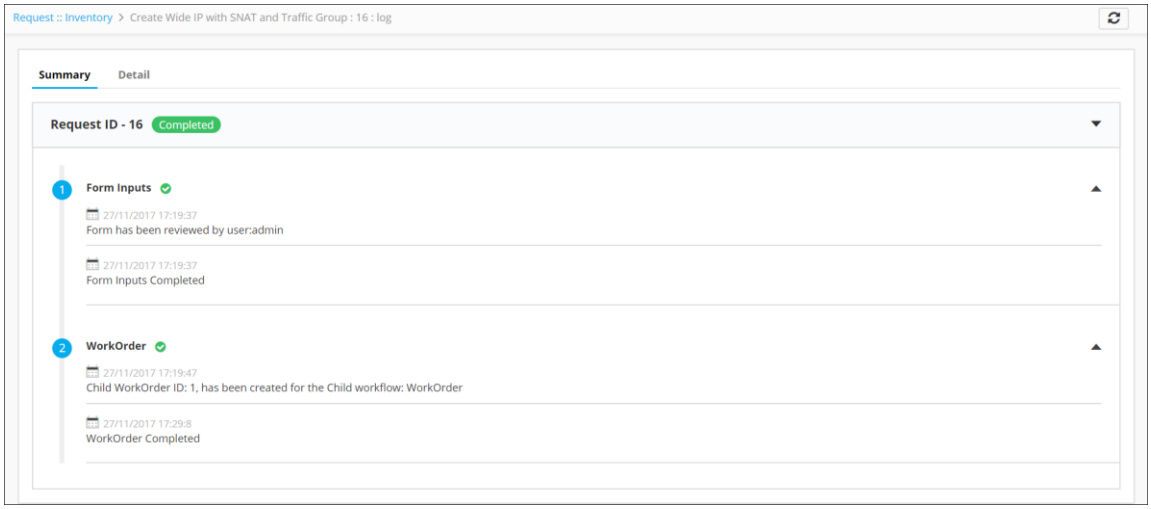
1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   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 Create Wide IP with SNAT and Traffic Group 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 Create Wide IP with SNAT and Traffic Group workflow.
4. On the Create Wide IP with SNAT and Traffic Group 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 Create Wide IP with SNAT and Traffic Group 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.