AppViewX

Delete WideIP F5 and Citrix Workflow Guide

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

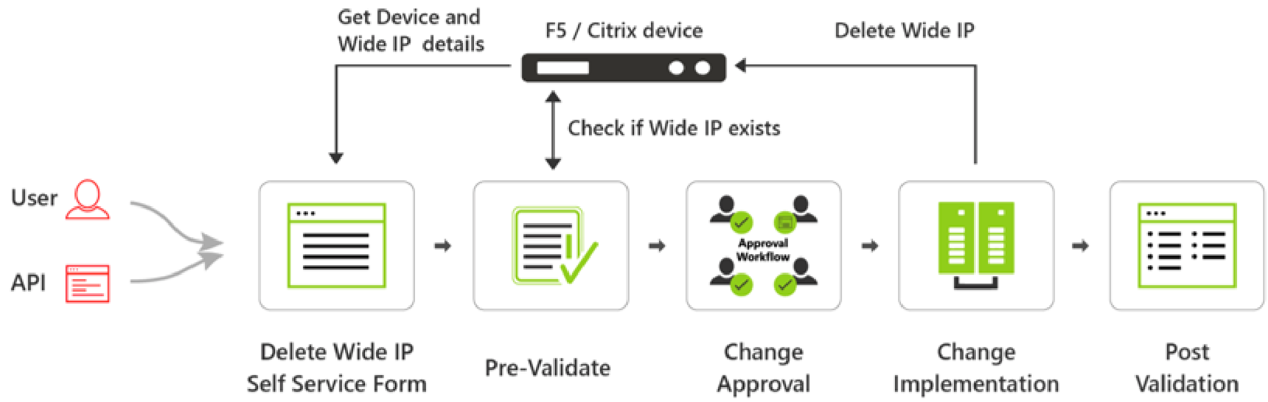
Contents

Description

The Delete WideIP F5 and Citrix workflow is used to delete a WideIP and its associated objects such as pool, pool members, profiles and monitors from the F5 and Citrix devices. This workflow displays the list of F5 and Citrix ADC devices and its associated WideIP(s) based on the user's access permissions, defined by Role Based Access Control (RBAC). The configurations to delete the WideIP and its associated objects are reviewed and approved at AppViewX. After the approval is granted, the WideIP and its unused dependent objects will be deleted.

Note: The dependent objects are deleted only if those objects are not associated with another virtual server.

The Delete WideIP F5 and Citrix 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.
- Each ADC device is a managed entity in AppViewX.
- You have administrator permissions to add a device to the AppViewX inventory.

Compatible Software Versions

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

- AppViewX – Free AppViewX, AVX 12.1.0, and AVX 12.2.0
- F5 (both LTM and GTM) – version 10.x, 11.x, or 12.x
- Citrix Device – ns version 11.0

Limitations

Not applicable

Log In to AppViewX

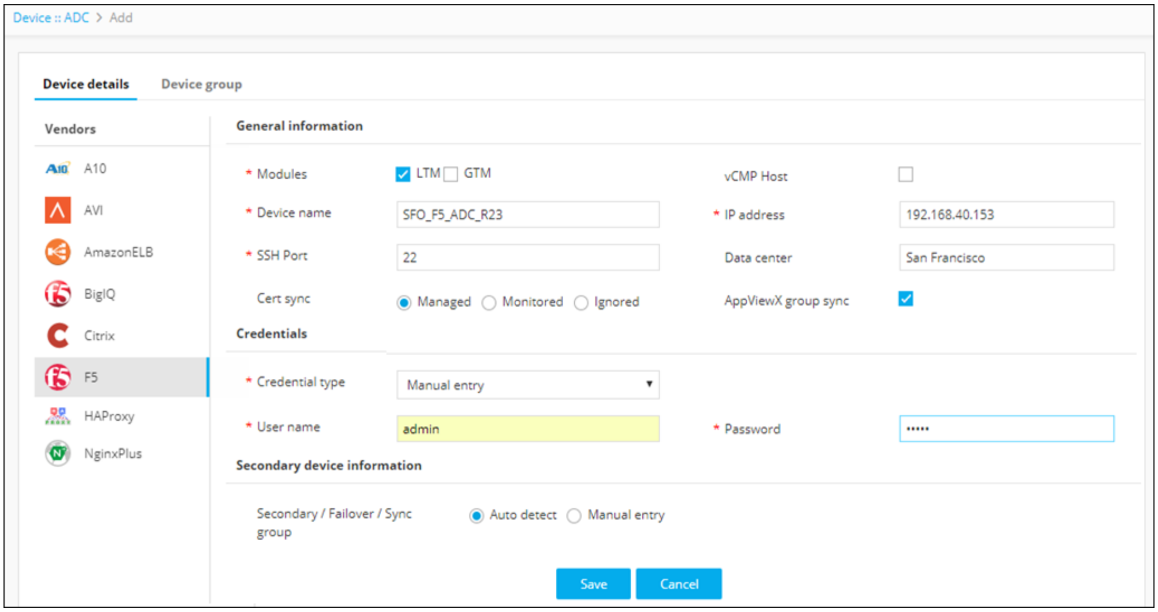
Log in to the AppViewX web interface. The standard format for a login URL is:
`https://hostname:portnumber`.

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 an ADC Device: F5 and Citrix

1. Click the (Menu) button.
2. Navigate to **Inventory** > **Device**.
3. The *Device* screen opens with the **ADC** tab displayed by default.
4. Click the + (**Add**) button in the Command bar.
5. On the *Add* screen that opens, click to select **F5** or **Citrix** 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 (applicable only for F5 vendor).
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. Enter the default or custom defined **SSH port** number for the device.
11. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
12. 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**.

13. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby ADC device.

    Note: This is required in older F5 versions like v10. The latest versions of F5 sync automatically.

14. From the **Credential type** dropdown list, select how you want to provide the credentials:
    a. Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.
    b. Select **Credential list** if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the [Add a Credential] section of this guide.

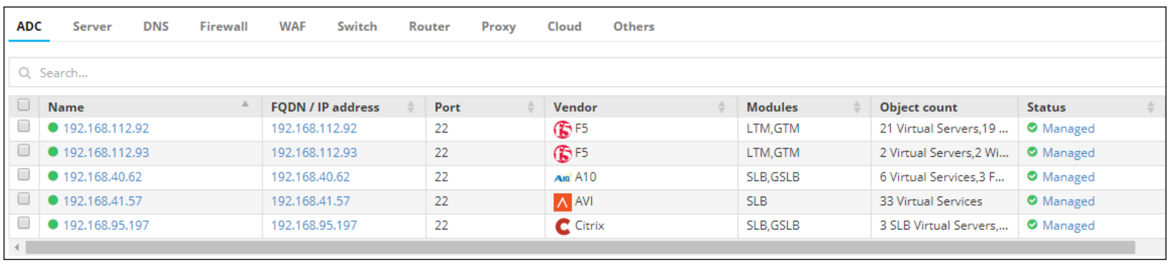
       When you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.

15. In the **Secondary/Alternate** device field, select how you want to fetch the details of a backup device when the primary device becomes unavailable due to failure or scheduled down time:
    a. Select **Auto detect** if you want AppViewX to automatically detect and retrieve the configuration of the secondary/alternate device, then click **Save** to add the device to AppViewX.
    b. Select **Manual entry** if you want to manually provide the details of the secondary device. At a minimum, fill in all fields that contain a red asterisk beside their names.

16. 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.

17. Click **Save** to add the new ADC device. The device is then displayed in the table on the **ADC** tab.



ADC Server DNS Firewall WAF Switch Router Proxy Cloud Others

Search...

Name	FQDN / IP address	Port	Vendor	Modules	Object count	Status
192.168.112.92	192.168.112.92	22	F5	LTM,GTM	21 Virtual Servers,19 ...	Managed
192.168.112.93	192.168.112.93	22	F5	LTM,GTM	2 Virtual Servers,2 Wi...	Managed
192.168.40.62	192.168.40.62	22	A10	SLB,GSLB	6 Virtual Services,3 F...	Managed
192.168.41.57	192.168.41.57	22	AVI	SLB	33 Virtual Services	Managed
192.168.95.197	192.168.95.197	22	Citrix	SLB,GSLB	3 SLB Virtual Servers,...	Managed

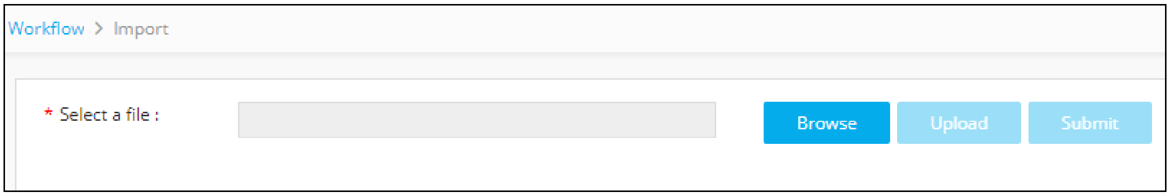
The device will display one of the following statuses:

- **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.

Import Visual Workflows

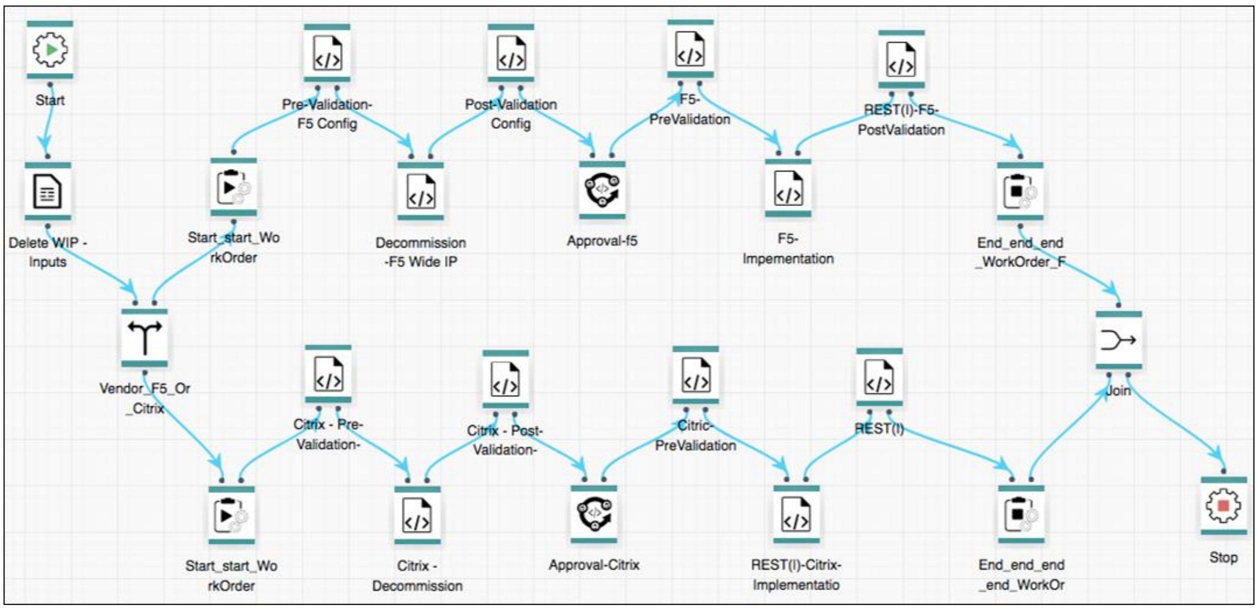
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows are available.

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 Delete WideIP F5 and Citrix workflow is shown in the image below:

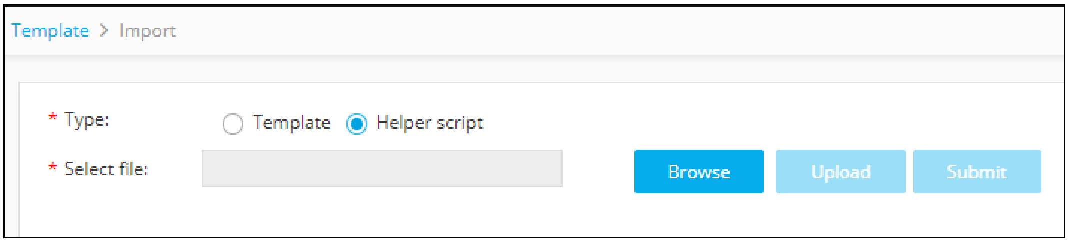


Import Helper Scripts

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.

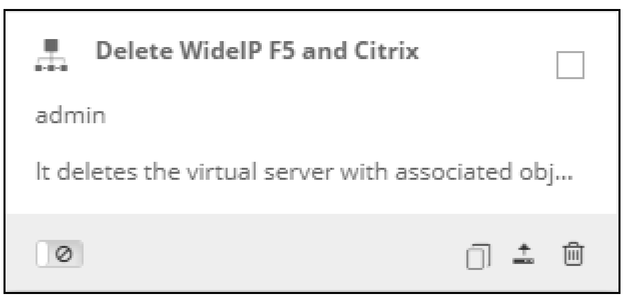
Enable a Workflow

To enable the Delete WideIP F5 and Citrix 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 Delete WideIP F5 and Citrix 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 Delete WideIP F5 and Citrix workflow from the Card view by clicking the (**Disable**) button.



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

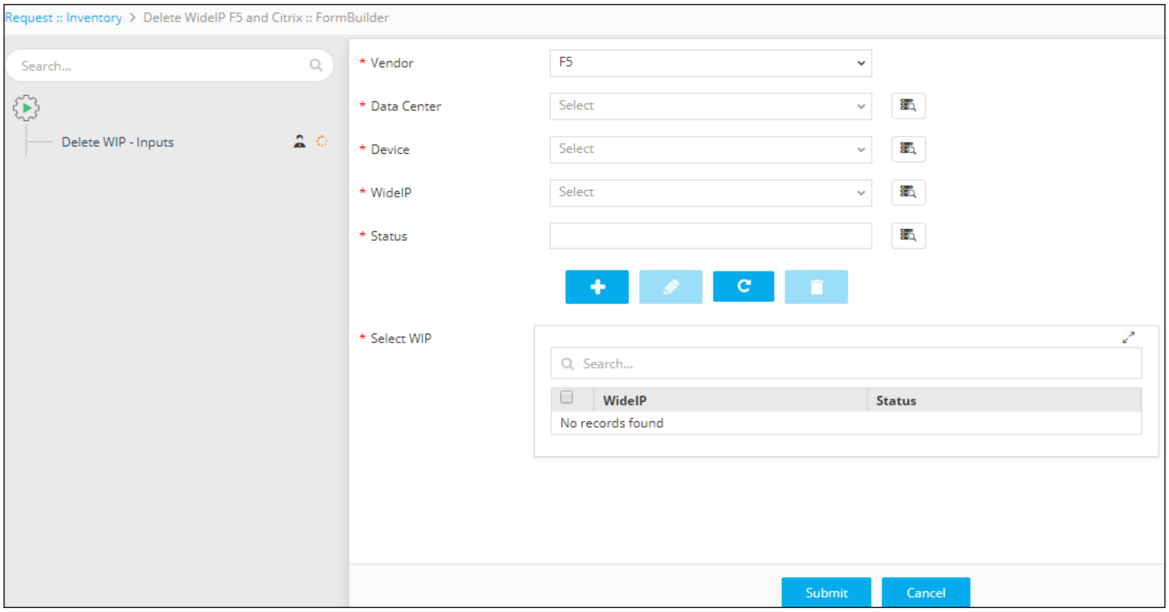
Delete WideIP F5 and Citrix workflow

To submit the Delete WideIP F5 and Citrix 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 to delete the WideIP.

   The *Form Builder* screen opens.



4. In the **Vendor** dropdown list, select the vendor from which you want to delete the WideIP.
5. In the **Data Center** field, retrieve the list of data centers that are added to the AppViewX inventory by clicking the (**Retrieve field values**) button and select the data center from the dropdown list.
6. In the **Device** field, retrieve the list of devices available in the selected data center by clicking the (**Retrieve field values**) button and select the required device from the dropdown list.
7. In the **WideIP** field, retrieve the list of WideIP(s) available in the selected device by clicking the (**Retrieve field values**) button and select the WideIP that you want to delete from the device.
8. In the **Status** filed, the status of the WideIP from the AppViewX inventory is retrieved and auto populated by clicking the (**Retrieve field values**) button.
9. Click the (**Add**) button to add the WideIP that you want to delete in the **Select WideIP** box.

   Note:

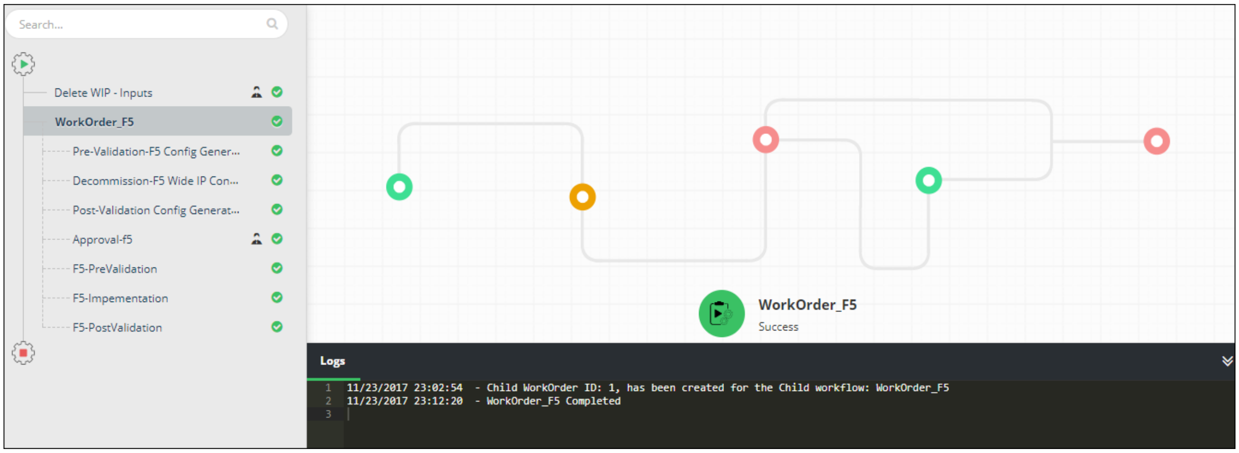
   - You can add one or more WideIP to the Select WideIP box.
   - You can also Update, Reset, and Delete a WideIP.
10. Click **Submit**.

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

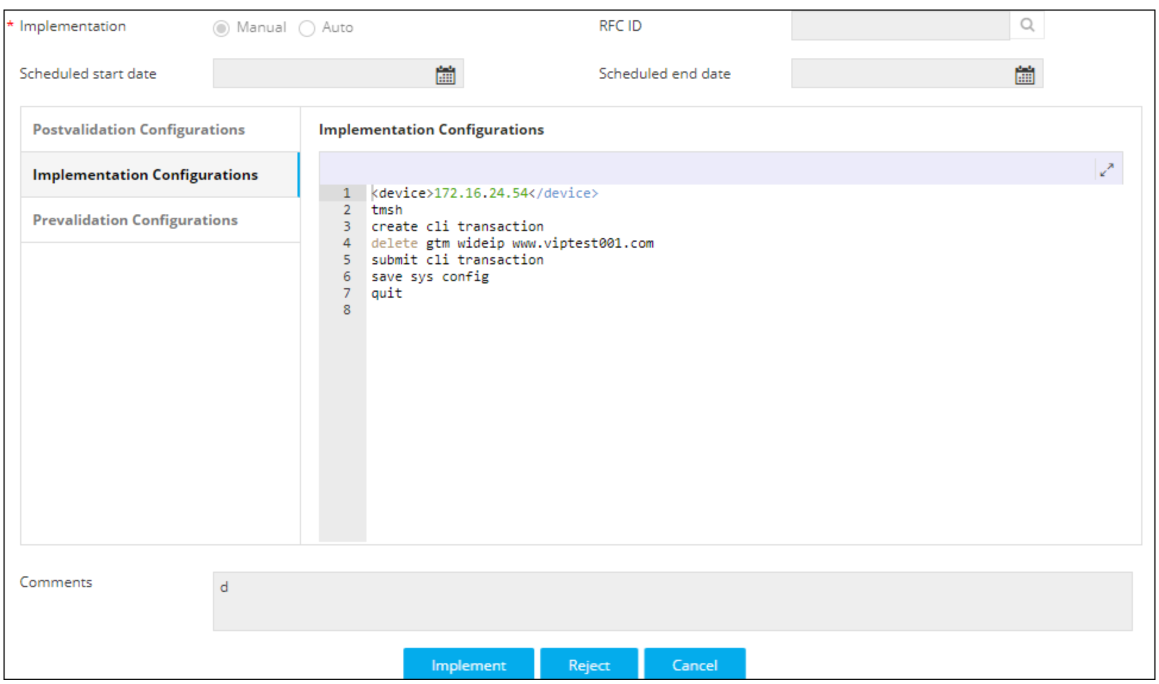
WorkOrder flow

The following are the workorder tasks for the Delete WideIP F5 and Citrix 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. **Pre-Validation-F5 Config Generation –** Configuration commands are generated to initiate the pre-validation process.
2. **Decommission-F5 Wide IP Config Generation –** Configuration commands are generated to initiate the decommission process.
3. **Post-Validation Config Generation –** Configuration commands are generated to initiate the post-validation process.
4. **Approval-F5 –** 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 commands are reviewed and approved at AppViewX. The configuration changes are implemented on the device only after approval is received.



   a. On the screen that opens, select **Manual** or **Auto** radio button depending on how you want to set the implementation process.

   b. If you have selected the **Auto** radio button, fill in all the fields, which are designated by red asterisk (*) beside their names.
   c. Enter any comments you have related to the post validation, implementation, and pre validation configuration request and then, click **Implement**.
5. **F5 Pre-validation –** Check the following:
   a. A list of WideIP(s) available in the source device.
   b. The performance metrics, such as CPU and memory utilization on the destination device, have been validated.
6. **F5 Implementation –** Configuration commands are implemented to delete the WideIP from the device you selected.
7. **F5 Post-Validation –** Checks if the WideIP you deleted is not present in the source device.

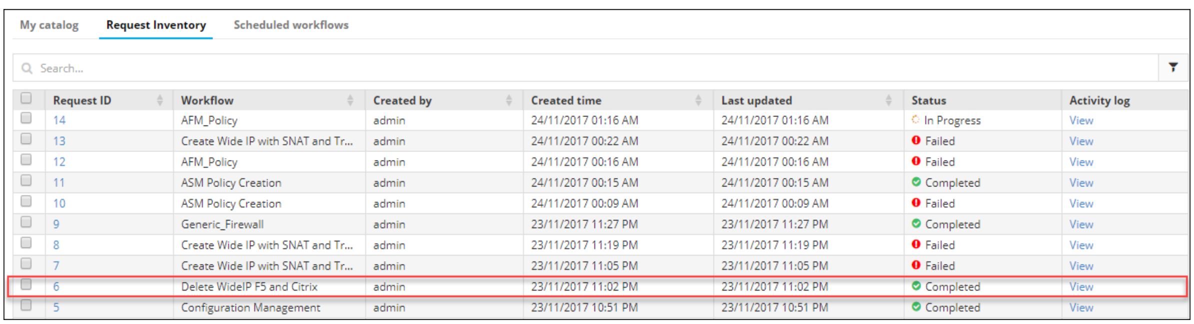
Request Inventory

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.



Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
14	AFM_Policy	admin	24/11/2017 01:16 AM	24/11/2017 01:16 AM	In Progress	View
13	Create Wide IP with SNAT and Tr...	admin	24/11/2017 00:22 AM	24/11/2017 00:22 AM	Failed	View
12	AFM_Policy	admin	24/11/2017 00:16 AM	24/11/2017 00:16 AM	Failed	View
11	ASM Policy Creation	admin	24/11/2017 00:15 AM	24/11/2017 00:15 AM	Completed	View
10	ASM Policy Creation	admin	24/11/2017 00:09 AM	24/11/2017 00:09 AM	Failed	View
9	Generic_Firewall	admin	23/11/2017 11:27 PM	23/11/2017 11:27 PM	Completed	View
8	Create Wide IP with SNAT and Tr...	admin	23/11/2017 11:19 PM	23/11/2017 11:19 PM	Failed	View
7	Create Wide IP with SNAT and Tr...	admin	23/11/2017 11:05 PM	23/11/2017 11:05 PM	Failed	View
6	Delete WideIP F5 and Citrix	admin	23/11/2017 11:02 PM	23/11/2017 11:02 PM	Completed	View
5	Configuration Management	admin	23/11/2017 10:51 PM	23/11/2017 10:51 PM	Completed	View

4. Click the **Request ID** created for Delete WideIP F5 and Citrix 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 Delete WideIP F5 and Citrix 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.