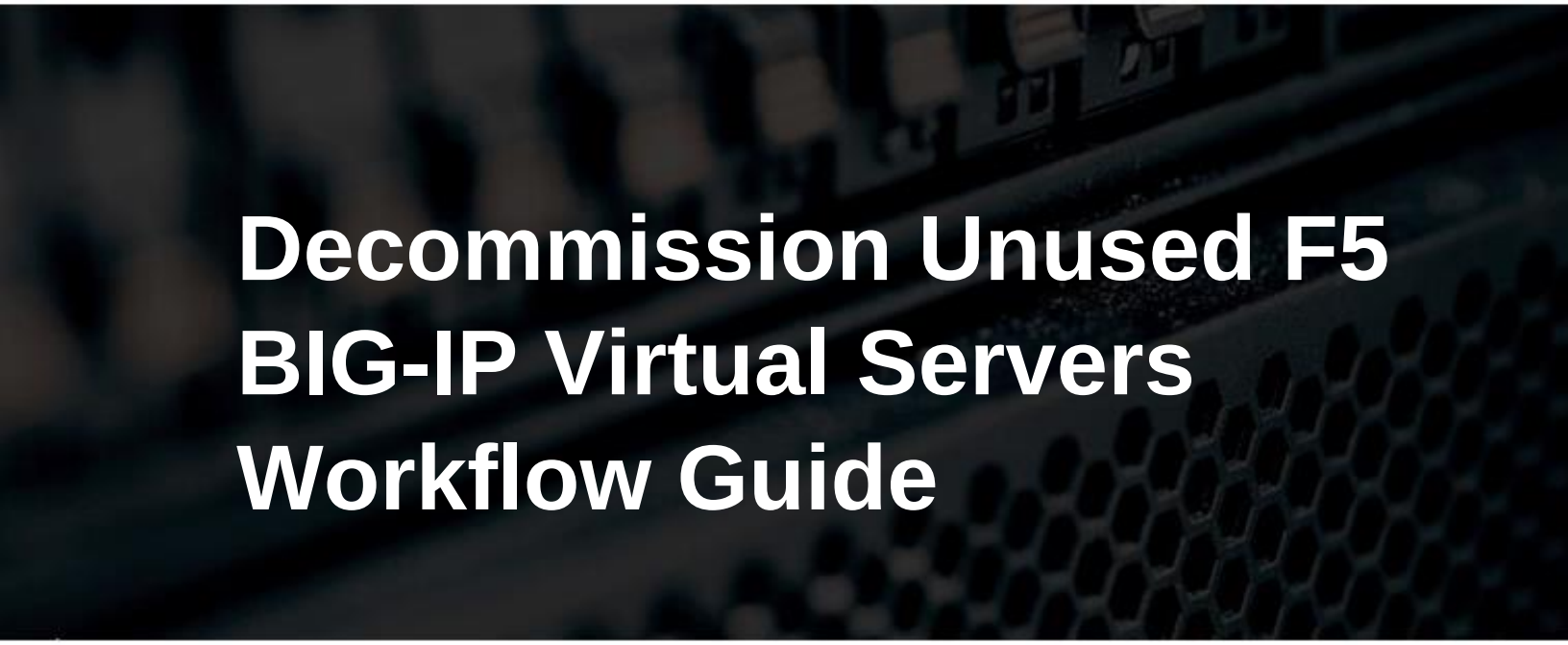
AppViewX



Decommission Unused F5 BIG-IP Virtual Servers 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: 12.3.0

Document Version: 1.0

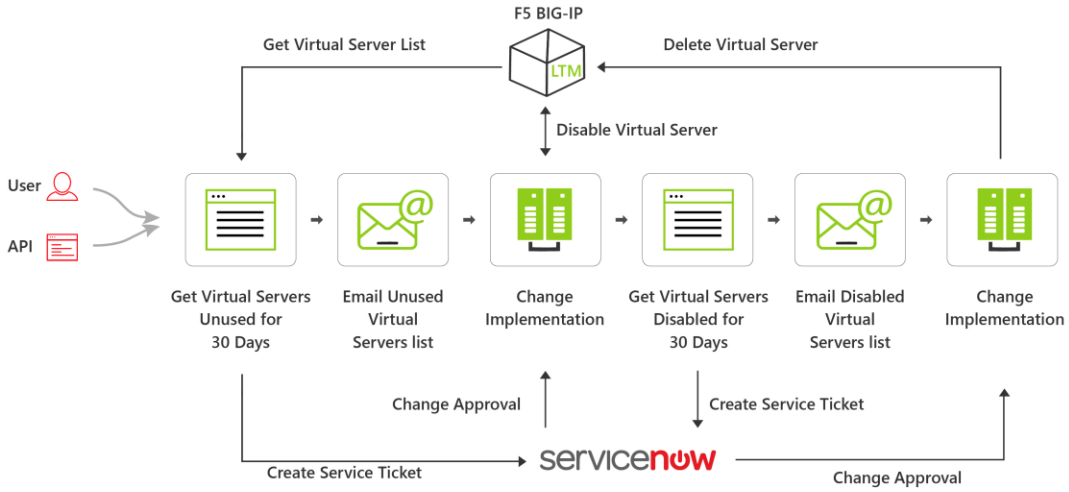
Last Updated on: July 26, 2018

Contents

1 Description

Decommission Unused F5 BIG-IP Virtual Servers workflow purges the virtual server and associated object configurations of applications, which are unused for 30 days or more from the managed F5 BIG-IP devices. Also, it provides an option to integrate with an ITSM tool such as ServiceNow for tracking and approval.

The flow diagram of the *Decommission Unused F5 BIG-IP Virtual Servers* workflow is as follows:



The workflow lists the virtual servers unused for 30 or more days based on the total number of client connections. The network admin is provided an option to select the unused virtual servers for disabling. The workflow pre-validates the virtual servers exist and generates the configurations to disable the selected virtual servers and the associated objects. On successful pre-validation, the configuration changes are reviewed and approved either at AppViewX or ServiceNow based on the selection of ITSM integration. On approval, the configuration changes are implemented on the device. Post-validation checks the virtual server and if the associated objects are successfully disabled. The report of disabled virtual servers is emailed to the ADC network admin.

The request will further wait for another 30 days to check if the state of disabled virtual servers changes. The network admin is provided an option to select the disabled virtual servers for deleting. The workflow pre-validates the virtual servers exist and generates the configurations to delete the selected virtual servers and associated objects, which are not used or shared with other virtual servers. On successful pre-validation, the configuration changes are reviewed and approved either at AppViewX or ServiceNow based on ITSM integration selection. On approval, the configuration changes are implemented on the device. Post-validation checks if the virtual server and associated objects are deleted. The deleted virtual servers report is emailed to the ADC network admin.

The following virtual server associate objects are decommissioned:

- Monitors

- Primary profiles (persistence profile, protocol profile, HTTP profile, FTP profile, client and server SSL profile, OneConnect profile, and Web acceleration profile)
- Pools
- Pool members
- Nodes
- SNAT Objects

2 Prerequisites

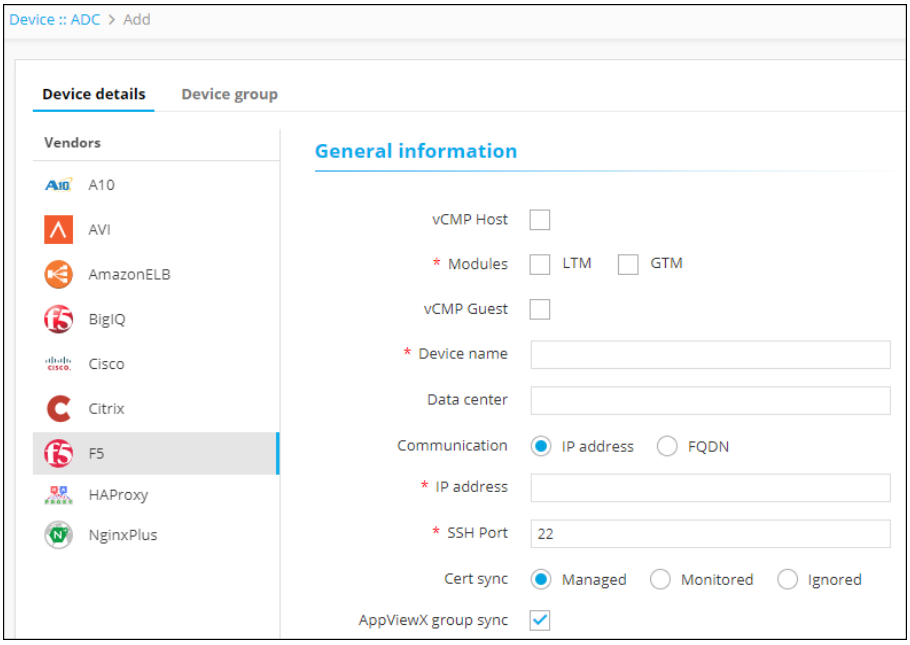
To run this workflow in your environment, the following prerequisites must be met:

- Free AppViewX or AppViewX 12.3 is downloaded and installed.
- F5 LTM devices are added to AppViewX ADC inventory as a managed device.
- SMTP server has been configured under System settings to receive email notifications.
- The recipient email IDs are updated in the *smtp_config* helper script.
- (Optional) ServiceNow is configured under change management section of AppViewX Settings.
- To capture the usage statistics of the ADC objects, select the vendor and objects of interest under **Settings** > **ADC** > Statistics.

2.1 Add an ADC Device: F5

To add a device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Inventory** > **Device**.
3. The *Device* screen opens with **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. Click the **vCMP Host** check box, if you want to add and manage the host devices.
7. Select the module LTM to be managed on the ADC device inventory.
8. Click the **vCMP Guest** check box, if you want to add and manage the guest devices.
9. Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
10. Select the **IP address** or **FQDN** radio button based on how you want to establish the communication.

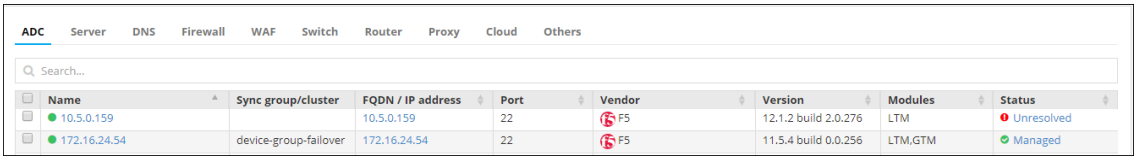
    Enter the IP address or FQDN in their corresponding fields depending on what you selected.
11. Enter the SSH port number of the device.
12. Specify a **Data center location** if you want to have the option later to filter devices based on their location.

    Note: Ensure that you provide the data center name, else the workflow cannot fetch the data center from where the device are selected.
13. 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**.
14. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby ADC device.

    This is required in older F5 versions like v10. The latest versions of F5 sync automatically.
15. From the **Credential type** dropdown list, select how to 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 **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 will be auto-filled with the values provided in the credential template.
16. 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.
17. Click **Add** to add the secondary device to the list at the bottom of the screen.

    Note: You can add more than one secondary devices. The **Update** and **Delete** buttons are enabled only when you try to modify the existing secondary device.
18. Click **Save** to save the new device in the table on the ADC tab.



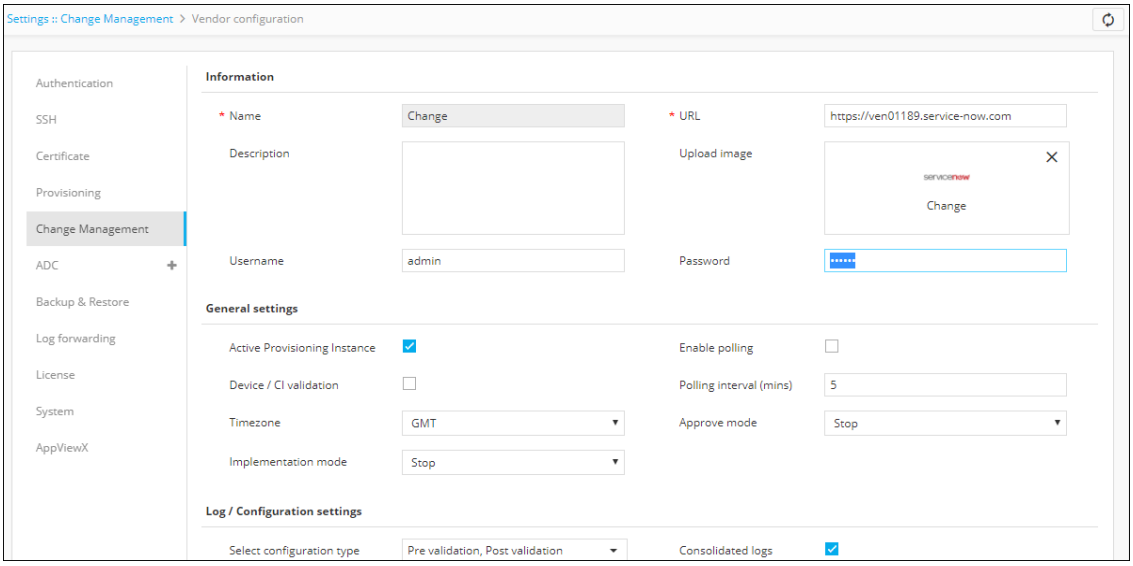
The device will display one of the following statuses:

- **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.

2.2 Register an ITSM Device: ServiceNow

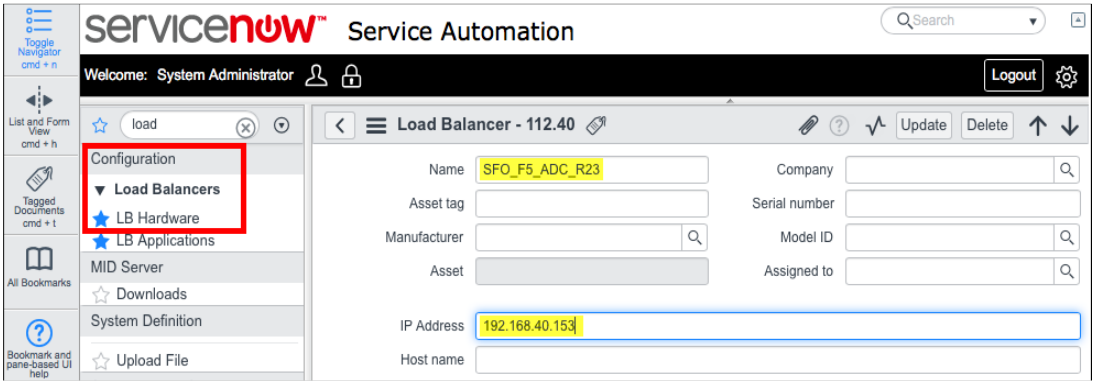
To configure the ITSM device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Settings** > **Change Management**.
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.



Note: Ensure that **Device/CI validation** check-box is deselected.

8. 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.



3 Compatible Software Versions

The application provisioning automation temples have been validated for the following software versions:

- AppViewX – FreeAppViewX and 12.3.0
- ServiceNow – Jakarta and Kingston
- F5 LTM – version 11.X, 12.X, or 13.X

4 Limitations

- The F5 BIG-IP device should be added as managed device in AppViewX inventory for minimum 30 days to get the unused Virtual servers data.
- There is no provision to delete Virtual Server DNS entries.
- The disabled Virtual Servers are also queuing for a disable again.

5 Log In to AppViewX

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

The default web credentials are set to `admin/AppViewX@123`.

Note: It is recommended that you access AppViewX using Internet Explorer (Version 11.0.9600.18817), Firefox (Version 59.0) or Google Chrome (Version 64.0.3282.186).

6 Preliminary Tasks

Following are the preliminary tasks that needs to be performed before executing a workflow:

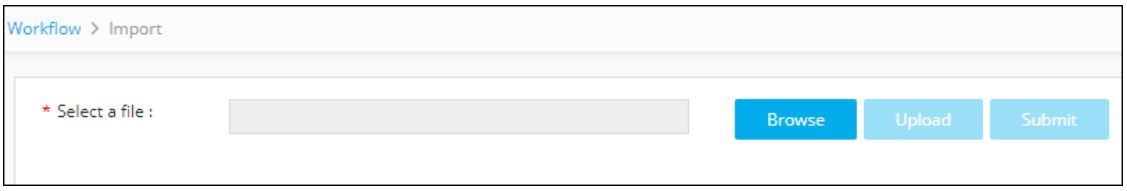
- Import a Workflow
- Import a Helper Script
- Enable a Workflow

6.1 Import a Workflow

To import the workflow, complete the following steps:

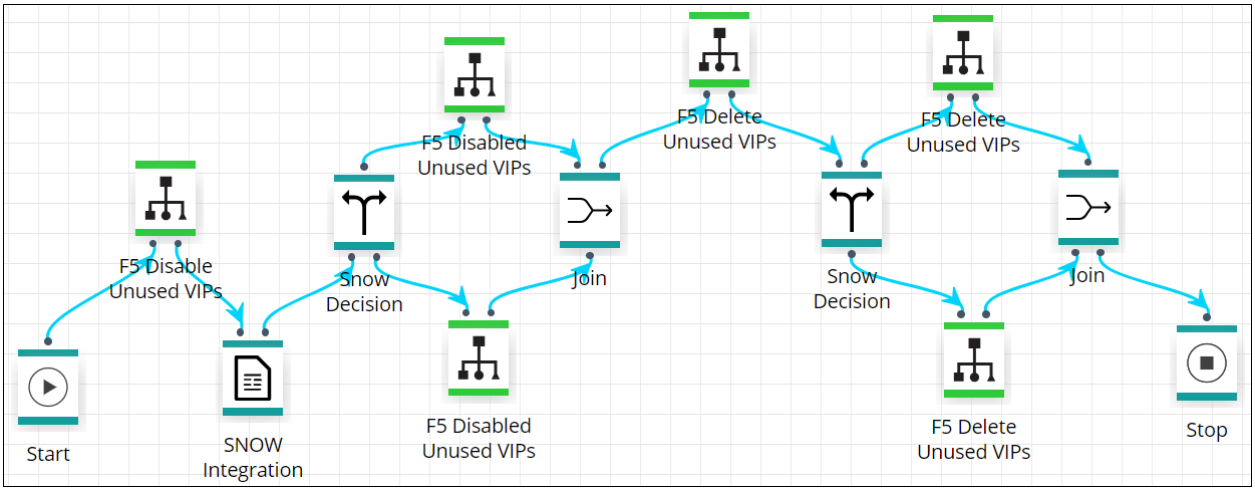
1. Click the (**Menu**) button.
2. Navigate to **Workflow > Studio**.

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.

The *Decommission Unused F5 BIG-IP Virtual Servers* workflow is shown in the image below:

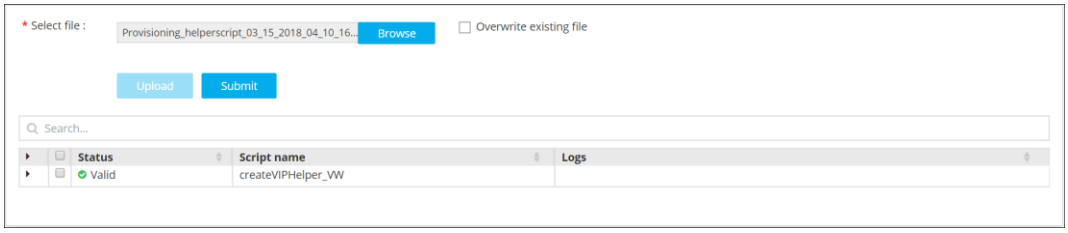


You can modify the vendors of ADC devices. For more details on how to modify the vendors, refer to the **Error! Reference source not found.** section in this guide.

6.2 Import a Helper Script

To import a helper script, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click on the (**Helper script**) button. The *Helper script library* screen appears.
4. Click the (**Import**) button.
5. Click **Browse** and select the helper script zip file you want to import.
6. Click **Upload** to import the file and view its contents.



Note: Select the checkbox **Overwrite existing file**, only if the names of the new script file that you are trying to upload and the existing script file are the same.

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

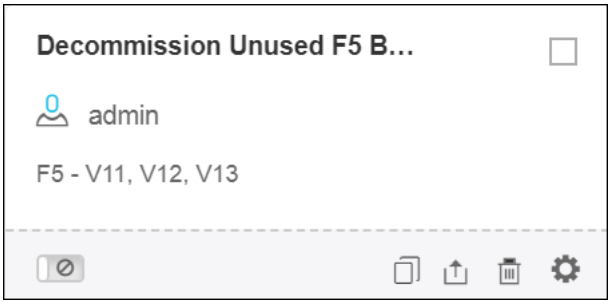
6.3 Enable a Workflow

To enable the 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 *Decommission Unused F5 BIG-IP Virtual Servers* workflow to enable it. 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 required workflow from the Card view by clicking the (**Disable**) button.



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

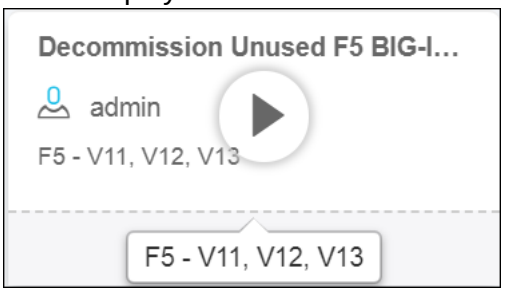
7 Decommission Unused F5 BIG-IP Virtual Servers

To execute the *Decommission Unused F5 BIG-IP Virtual Servers* workflow, complete the following steps:

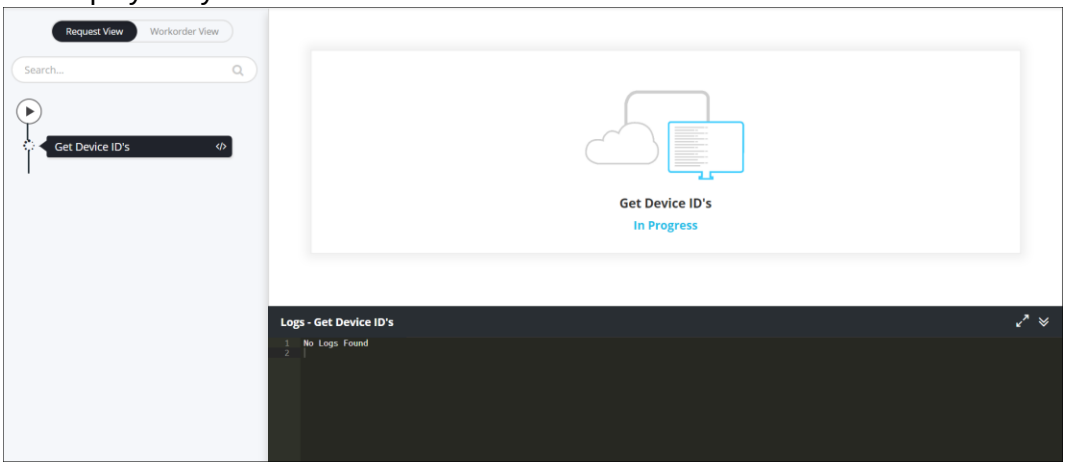
1. Log in to AppViewX using the application owner credentials.
2. Click the (**Menu**) button.
3. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default. This screen displays all enabled workflows assigned to a specific user role.

4. Click the play button on the *Decommission Unused F5 BIG-IP Virtual Servers* workflow.



5. The **Decommission Unused F5 BIG-IP Virtual Servers** opens with the **Request View** tab displayed by default.



6. **Get Device IDs** of the F5 devices managed in the AppViewx system.
7. **Get Unused VIPs:** An API is triggered to get the details of unused object from the device ID retrieved in step 6.
8. **Grid** displays a table with the device name, VIP name, and the number of days it has remained unused.
9. **Get VIP Details:** Retrieves the partition and state detail of each VIP.
10. **Get Unused VIPs List:** Retrieves the VIP details, which have not used for 30 or more days.
11. **unused_vip_mail_script:** Generates the email content with the unused VIP details.
12. **Notification Inputs:** The notification inputs form will list the details of the VIP that will be disabled.
13. **Generate Disable Commands:** Generates the config commands to disable the VIP and push it to the respective device on which it resides.
14. **SNOW Integration:** Provides an option to create an ITSM ticket.
15. If **Yes** was selected in step 14, select the following details of the ticket:
    - **Start date and time**
    - **End date and time**
16. If SNOW integration was opted in step 14, the flow will be as follows:
    a. **Create Ticket:** The SNOW ticket is created with the selected start and end date.
    b. **Get Ticket Details:** Get the created ticket sysID, which is used to update the ticket in the later stages.
    c. **Push Config:** Push the change plan detail to the created ticket.
    d. **Convert date to Milliseconds:** Convert the start and end time to milliseconds.

e. **Schedule:** Allow the workflow to poll the ticket between start and end time to check if it is approved.
f. **Validate Ticket Status:** Check and get the status of the ticket.
g. **Retry:** Poll the ticket status every 5 seconds between the start and end dates.
h. **Approval:** Second level of approval for the reviewer to validate the config commands and to implement or reject the configuration.
i. **Implementation:** The configuration is pushed to the device.
j. **Close Complete:** The ticket is closed as implemented.
k. **Close Incomplete:** The ticket is closed as not implemented.
l. **SNOW mail script:** The email content is generated with the CSV file for the VIPs that are unused for more than 30 days.

17. If SNOW integration was not opted in step 13, the flow will be as follows:
    a. **Approval:** The second level of approval for the reviewer to validate the config commands and to implement or reject the configuration.
    b. **Implementation:** The configuration is pushed to the device.
    c. **Disabled VIP Mail Script**: The email content is generated with the CSV file for the VIPs that are unused for more than 30 days.
18. **Schedule**: Wait for 30 days from the date of disabling the selected VIP.
19. **Get Device IDs** of the Citrix devices managed in the AppViewx system.
20. **Get Unused VIPs:** An API is triggered to get the details of unused object from the device ID retrieved in step 18.
21. **Get VIP Details:** Retrieves the partition and state detail of each VIP.
22. **Get Unused VIPs List:** Get a detailed list of the VIPs, which are disabled for more than 30 days.
23. **VIP Check:** Checks whether the disabled VIP was enabled during the 30 days after being disabled.
24. If any VIPs are available for deleting, the flow will be as follows:
    a. **Generate VIP Validation Commands:** Generate the prevalidation commands for the deleting the VIP.
    b. **Generate VIP Decommissioning Commands:** Generate the commands for deleting the VIP, it generate the VIP, service group, servers, and monitors.
    c. **Generate VIP Rollback Commands:** Generate the VIP rollback commands, which are deleted in the forward flow. It recreates the deleted objects such as VIP, service group, server, and monitors.
    d. **Mail Script:** Triggers an email with the details of the VIP.
25. If SNOW integration was opted in step 14, the flow will be as follows:
    a. **Ticketing Inputs:** Select the following details:
        - **Start date and time**
        - **End date and time**
    b. **Create Ticket:** The SNOW ticket is created with the selected start and end date.
    c. **Get Ticket Details:** Get the created ticket sysID, which is used to update the ticket in the later stages.
    d. **Push Config:** Push the change plan detail to the created ticket.
    e. **Convert date to Milliseconds:** Convert the start and end time to milliseconds.
    f. **Schedule:** Allow the workflow to poll the ticket between start and end time to check if it is approved.

g. **Validate Ticket Status:** Check and get the status of the ticket.
h. **Check Ticket Approval :** Based on the status returned in the previous step:
    - If approved, move to the Approval stage
    - If requested, move to the Retry stage.
    - If withdrawn, move to the Close incomplete stage.
i. **Retry:** Poll the ticket status every 5 seconds between the start and end dates.
j. **Approval:** Second level of approval for the reviewer to validate the config commands and to implement or reject the configuration.
k. **Execute Prevalidation:** The prevalidation commands are executed.
l. **Execute Delete VIP Commands:** The configuration is pushed to the device.
m. **Execute Postvalidation:** The postvalidation commands are executed.
n. **Close Complete:** The ticket is closed as implemented.
o. **Close Incomplete:** The ticket is closed as not implemented.

26. If SNOW integration was not opted in step 14, the flow will be as follows:
    a. **Approval:** Second level of approval for the reviewer to validate the config commands and to implement or reject the configuration.
    b. **Execute Prevalidation:** The prevalidation commands are executed.
    c. **Execute Delete VIP Commands:** The configuration is pushed to the device.
    d. **Execute Postvalidation:** The postvalidation commands are executed.

8 Rollback a Workorder

A rollback action can be performed only on the completed workflows. To trigger a rollback action, 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 **Request Inventory** tab.
5. This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request created for *F5 VIP Decommission* workflow using the **Search** field and/or click the  (**Filter**) button.
6. Right-click the request and select **Rollback**.
7. On the Confirmation screen that appears, click **Yes**.
8. Select the **Request** or **Workorder** radio button based on how you want to set the rollback type.
9. Click **Rollback** to trigger the action.

8.1 Workorder Flow

The following are the workorder tasks of *Decommission Unused F5 BIG-IP Virtual Servers* 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. **Approval** – Review of a work order is based on the role assigned to the user, who has 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 after approval is received.
2. **RollBack** – The configuration commands are rolled back, resulting in the recreation of the virtual server and the associated LTM object, which were deleted in the forward flow.

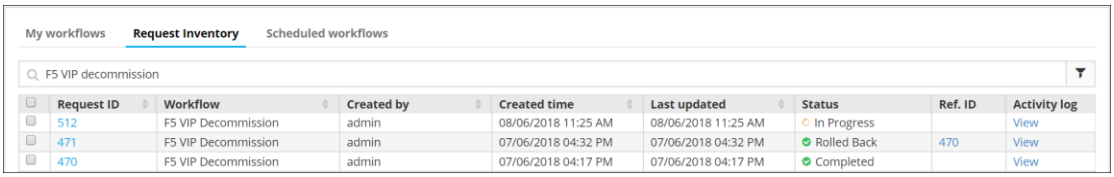
9 Request Inventory

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

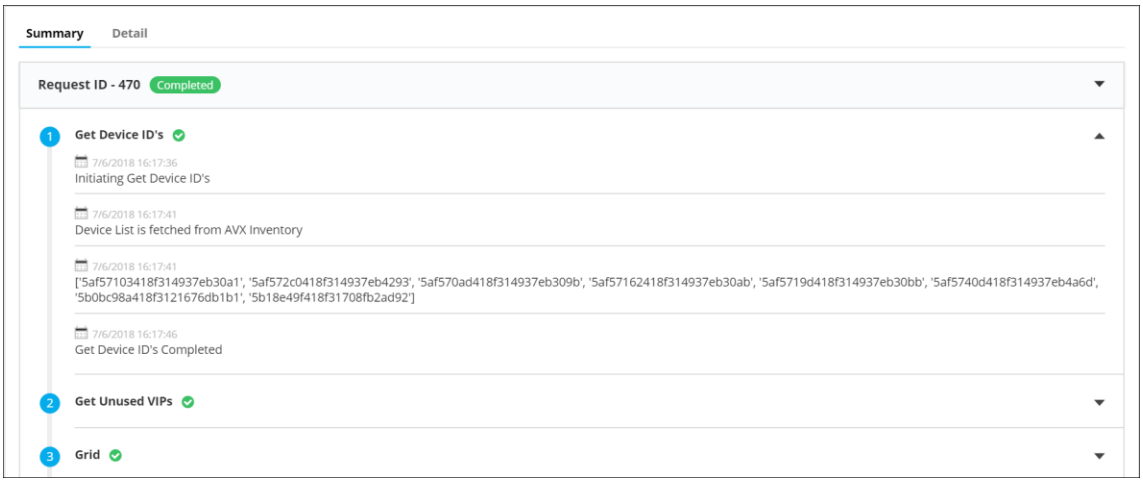
1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   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** of the requested workflow to view the tasks or phases of a request in a tree-view.
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.



10 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 respective workflow.
4. On the 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 the selections you make.
5. Click **Save**.

11 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.

12 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 respective 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.

13 Troubleshooting

I cannot find the 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.