



Create Virtual Server Workflow Guide

Copyright © 2018 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 VMware, Inc. (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 (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: April 05, 2018

Contents

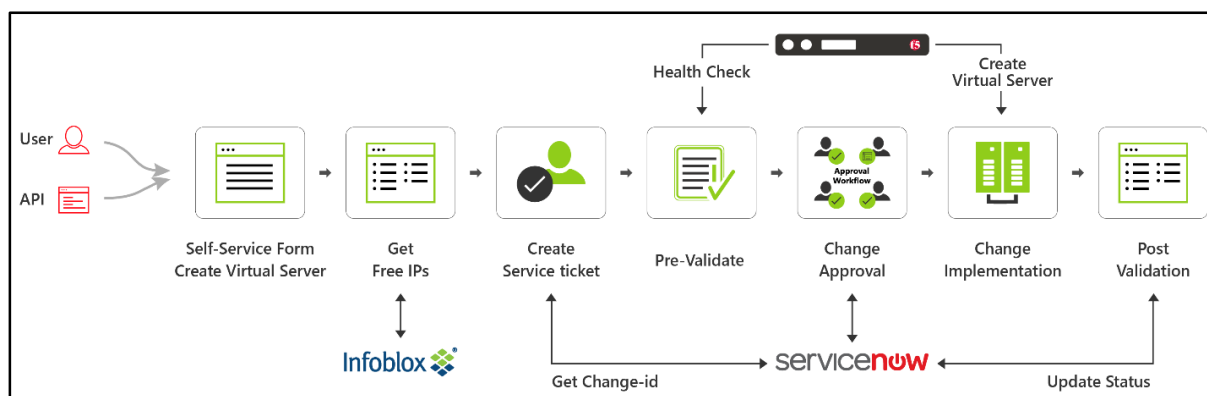
AppViewX Overview.....	1
Create Virtual Server Workflow	2
Prerequisites	2
Compatible Software Versions	2
Application Provisioning Tasks.....	3
Log In to AppViewX	3
Import Visual Workflows.....	3
Import Helper Scripts	4
Add an ADC Device: F5 LTM	4
Add an IPAM Device: Infoblox.....	6
Register an ITSM Device: ServiceNow	7
Enable a Workflow	8
Create a Virtual Server Workflow	8
Workorder Flow.....	11
Request Inventory	14
Schedule a Workflow	15
View Scheduled Workflows	15
Troubleshooting	15

AppViewX Overview

Application-oriented companies can only accomplish true business agility through the automation of delivery infrastructure. At AppViewX, we believe that in order to power faster and more compliant application provisioning, Network Operations groups need to work smarter, not harder. Our platform offers a solid foundation to start your automation journey. It enables complete change management automation by integrating with leading technology providers and defining workflows for all stages of application provisioning on ADC: validation, approval, implementation, and rollback. To get started, you can download Free AppViewX, which comes with a series of preloaded application automation provisioning workflows.

Create Virtual Server Workflow

The *Create Virtual Server* workflow creates a virtual server and associates it with profiles, monitors, pool, and pool members in F5 LTM using Infoblox and ServiceNow integration. It uses a simple, self-service based approach to gather application-provisioning requirements and generate vendor-specific configurations or REST APIs. This self-service workflow filters F5 ADC devices based on the user's access permissions, defined by Role Based Access Control (RBAC). The platform integrates with IP address management (IPAM) systems like Infoblox, which allows users to reserve a free IP address from the available address pools and create DNS binding for the new virtual server in Infoblox. The workflow also includes an option to create or bind existing profiles and monitors to the virtual server and allows users to create change request tickets in ITSM systems like ServiceNow for approvals and tracking. The service request change ID is associated with the work order and is updated based on the implementation status.



The work order pre-validates ADC device performance metrics (CPU and memory utilization) and confirms that the new virtual server and associated objects are not present. On successful pre-validation, the configuration changes are reviewed through a two-level approval process: first by ServiceNow, then by AppViewX. After approval is received, the configuration changes are implemented on the ADC device. A post-validation script ensures the virtual server and the associated objects are created successfully.

Prerequisites

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

- Free AppViewX or AVX 12.3.0 has been downloaded and installed.
- An F5 LTM device has been added to AppViewX as a managed device.
- (Optional) An Infoblox device has been added to AppViewX.
- (Optional) ServiceNow is registered to AppViewX.
- Multiple server nodes are running the application.

Compatible Software Versions

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

- AppViewX – Free AppViewX and AVX 12.3.0
- ServiceNow – Geneva, Eureka, Istanbul, and Jakarta

- Infoblox – version 7.2.X
- F5 LTM – version 10.X, 11.X, or 12.X

Application Provisioning Tasks

Within the AppViewX Provisioning module, you can perform a wide range of tasks, details of which are provided in this section.

Log In to AppViewX

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



`http://hostname:portnumber`

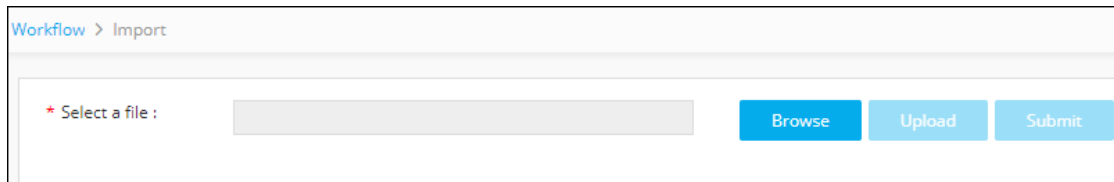
The hostname and port number are configured during deployment, with the default port number set to 5004 and the default web credentials set to `admin/AppViewX@123`.

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

Import Visual Workflows

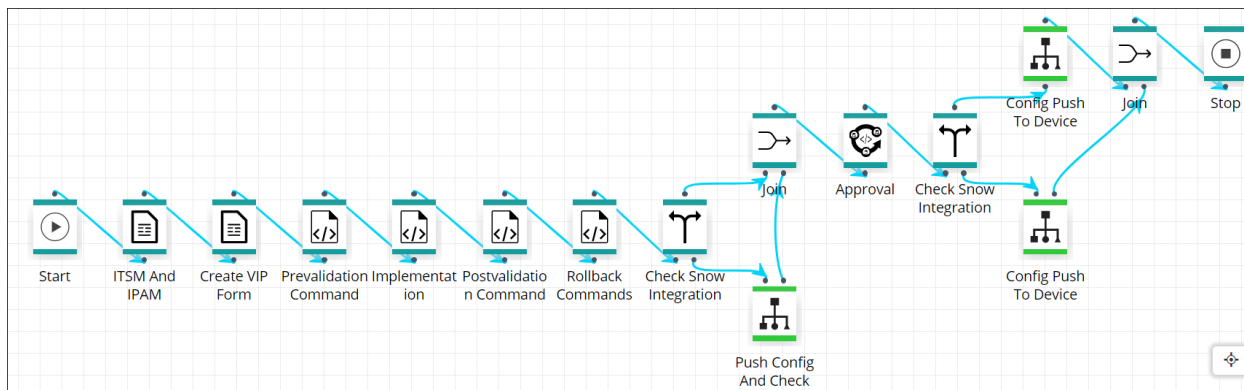
Note: Free AppViewX comes preloaded with visual workflows. You will only need to use the following import instructions when newer versions of the workflows become available.

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 Create Virtual Server 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 become available.

To import a helper script, complete the following steps:

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Workflow > Studio**.
2. Click on the (**Helper script**) button. The *Helper script library* screen appears.
3. Click the (**Import**) button.
4. Click **Browse** and select the helper script zip file you want to import.
5. Click **Upload** to import the file and view its contents.

* Select file : Provisioning_helperscript_03_15_2018_04_10_16... ☐ Overwrite existing file

Search...

Status	Script name	Logs
<input checked="" type="checkbox"/> Valid	createVIPHelper_VW	

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.

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

Add an ADC Device: F5 LTM

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Inventory > Device**.
2. On the *Device* screen, click the **ADC** tab if it is not already visible.
3. Click the (**Add**) button in the Command bar.
4. On the *Add* screen that opens, click to select **F5** as the ADC vendor.

The screenshot shows the 'Add Device' form in the AppViewX interface. The 'Device details' tab is active, and the 'Vendors' list on the left has 'F5' selected. The 'General information' section includes fields for 'Modules' (with 'LTM' checked), 'IP address' (192.168.40.153), 'Device name' (SFO_F5_ADC_R23), 'Data center' (San Francisco), 'Cert sync' (set to 'Managed'), and 'AppViewX group sync' (checked). The 'Credentials' section has 'Credential type' set to 'Manual entry', 'User name' as 'admin', and a masked 'Password'. The 'Secondary device information' section has 'Secondary / Failover / Sync group' set to 'Auto detect'. 'Save' and 'Cancel' buttons are at the bottom.

5. Select the module to be managed on the ADC device.
6. Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
7. Enter the **management IP address** of the device.
8. (Optional) Specify a **Data center location** if you want to have the option later to filter devices based on their location.
9. 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**.
10. (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.
11. Select a **Credential type** from the dropdown menu.
12. Enter the **User name** and **Password** that are associated with the credentials.
13. **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.

The screenshot shows the 'ADC' tab in the AppViewX interface. A table lists the devices. The newly added device 'SFO_F5_ADC_R23' is shown with status 'Managed'.


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

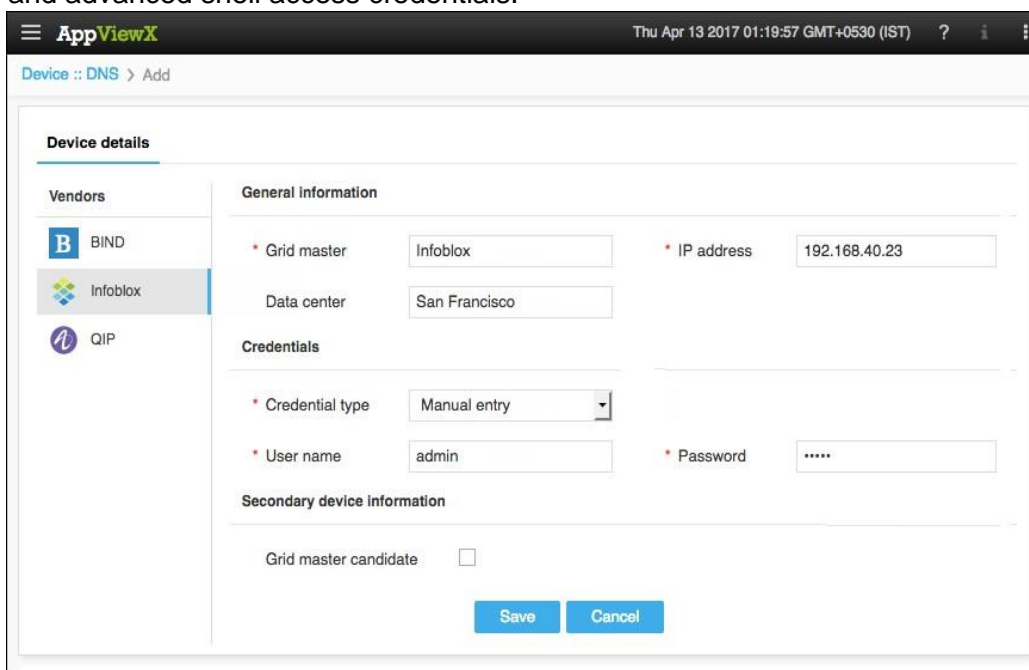
The device will display one of the following statuses:

- 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 IPAM Device: Infoblox

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Inventory > Device**.
2. Click the **DNS** tab.
3. Click the  (**Add**) button in the Command bar.
4. On the *Add* page that appears, click to select **Infoblox** and enter the device's IP address and advanced shell access credentials.



AppViewX Thu Apr 13 2017 01:19:57 GMT+0530 (IST)

Device :: DNS > Add

Device details

Vendors

- B BIND
- Infoblox
- QIP

General information

* Grid master: Infoblox

* IP address: 192.168.40.23

Data center: San Francisco

Credentials

* Credential type: Manual entry

* User name: admin

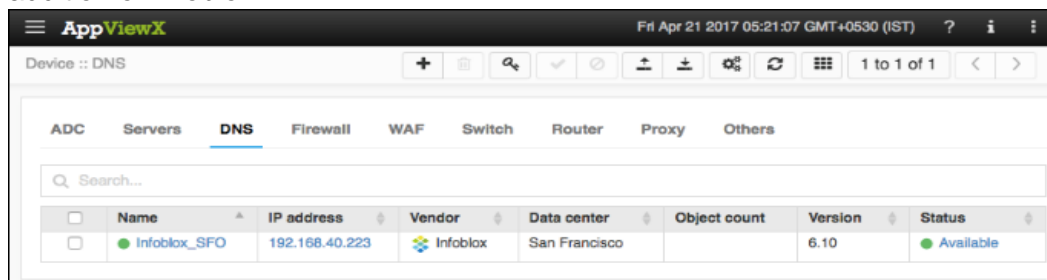
* Password:

Secondary device information

Grid master candidate: ☐

Save Cancel

5. Click the **Save** button.
- The device status on the DNS tab changes to **Available** to indicate the successful addition of Infoblox.



AppViewX Fri Apr 21 2017 05:21:07 GMT+0530 (IST)

Device :: DNS

ADC Servers **DNS** Firewall WAF Switch Router Proxy Others

Search...

	Name	IP address	Vendor	Data center	Object count	Version	Status
<input type="checkbox"/>	Infoblox_SFO	192.168.40.223	Infoblox	San Francisco		6.10	Available

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.

The screenshot shows the AppViewX Settings - Change Management - Vendor configuration page. The left sidebar contains a navigation menu with options: Authentication, SSH, Certificate, Provisioning, Change Management (selected), Device, Log forwarding, License, iHealth report, System, and AppViewX. The main content area is titled 'Vendor configuration' and includes the following sections:

- Information:**
 - Name: Change
 - Description: (empty text area)
 - URL: https://ven01189.service-now.com
 - Upload image: (empty image upload area)
 - Username: admin
 - Password: (masked with asterisks)
- General settings:**
 - Active Provisioning Instance: ☒
 - Device / CI validation: ☒
 - Timezone: GMT
 - Implementation mode: Override
 - Enable polling: ☒
 - Polling interval (mins): 5
 - Approve mode: Override
- Log / Configuration settings:**
 - Select configuration type: Pre validation, Post validation
 - Select log type: None selected
 - Consolidated logs: ☒
 - Auto close: ☒
- Configuration command:**

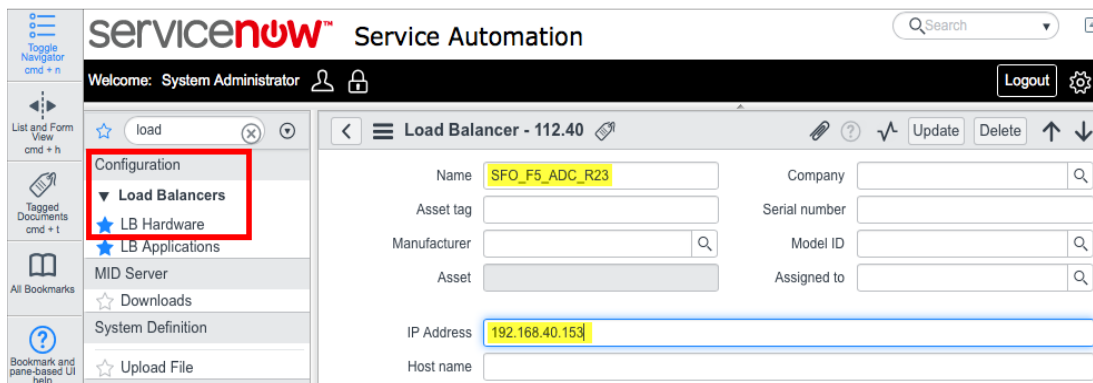
```

1 {
2   "serviceApiList": {
3     "create": {
4       "url": "/api/now/table/change_request",
5       "responseDataMapping": {
6         "ticketNumber": "result-number"
7       },
8       "payloadDataMapping": {
9         "start_date": "startTime",
10        "end_date": "endTime",
11        "work_notes": "data",
12        "close_notes": "description",
13        "cmdb_ci": "cmdb_ci"
14      },
15       "apiListToCallAfter": [],
16       "name": "createTicket",
17       "method": "POST"
18     },
19     "getTicket": {
20       "url": "/api/now/table/change_request?sysparm_query=number=ticketNumber",
21       "responseDataMapping": {
22         "state": "result-approval",
23         "startTime": "result-start_date",

```



At the bottom of the configuration command section are three buttons: Update, Reset, and Cancel.


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.

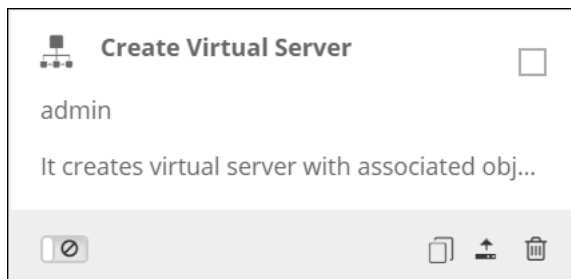


Enable a Workflow

To enable the *Create Virtual Server* workflow, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. The *Workflow* screen opens.
4. Click the ☐ (**Select**) button on the *Create Virtual Server* workflow to enable it. If the workflow is already selected, a ☒ (**Deselect**) button appears.
5. 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.




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

Create a Virtual Server Workflow


To submit the *Create Virtual Server* 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 *Create Virtual Server* workflow.
4. For the **Do you want to integrate IPAM**, select the **Yes** radio button. The self-service form fields are updated automatically based on the selection.
 - a. In the **Device** dropdown, select the required Infoblox device.



- b. In the **FQDN** field, enter a fully qualified domain name for the VIP.
 - c. Click the **Get Subnets** button to fetch the available list of subnets and then, select the required subnet from the **Subnet** dropdown.
 - d. Click the **Reserve Free IP** button to reserve a free IP address from the selected subnet. DNS binding is created for the virtual server with this IP address on Infoblox.
5. If ITSM integration is not required, select the **No** radio button. If it is required, select **Yes** and continue with the following steps:
 - a. Select the **Time Zone** of the F5 LTM device that you are configuring.
 - b. Schedule the maintenance window time and date using the **Start Date** and **End Date** fields. The configuration changes will be implemented during this maintenance window.
 - c. Click the  (**Retrieve field values**) button to create a new ServiceNow ticket and auto-populate the Change Request ID.
6. Click **Next**.
7. In the **F5 LTM Device** field, select the device on which the virtual server is to be created.
8. Enter a valid virtual server name in the **Virtual Server Name** field. The name should be suffixed with a valid DNS domain name.

Note: The parent domain specified in the App Name (FQDN) must be present in Infoblox to fetch the free IP address. If the domain is not present, the user will receive a warning message indicating failure to fetch the free IP address. Create the domain under the default DNS view in Infoblox.
9. Enter a virtual server IP in the **Virtual Server IP** field.
10. Enter the **Virtual Server Port** number used to access the application.
11. Click the **Fetch Device Details** button to retrieve virtual server related details from the selected device and populate the form fields, like profiles and monitors.
12. From the **iRules** dropdown, select one or more iRule(s) that must be associated to the VIP.

Note: If **None selected** is chosen, no client SSL profiles will get associated to the VIP.
13. From the **Client SSL Profile** dropdown, select one of the following options and complete the corresponding steps:
 - a. **Create New Client SSL Profile**
 - i. Click the **Fetch Client SSL Profiles** button to retrieve the SSL profiles from the selected device.
 - ii. Fill in the following details in the corresponding fields:
 - **Client SSL Profile Name**
 - **Client SSL Certificate**
 - **Client SSL Key**
 - **Client SSL Chain**
 - b. **Use Existing Client SSL Profile**
 - i. Click the **Fetch Client SSL Profiles** button to retrieve the SSL profiles from the selected device.
 - ii. From the **Select Client SSL Profile** dropdown, select the required client SSL profile.
 - c. **None:** If this option is selected, no client SSL profiles will be associated to the VIP.

14. From the **Server SSL Profile** dropdown, select one of the following options:
 - a. **Create New Server SSL Profile**
 - i. Click the **Fetch Client SSL Params** button to retrieve the SSL parameters from the selected device.
 - ii. Fill in the following details in the corresponding fields:
 - **Server SSL Profile Name**
 - **Server SSL Certificate**
 - **Server SSL Key**
 - **Server SSL Chain**
 - b. **Use Existing Server SSL Profile**
 - i. Click the **Fetch Server SSL Params** button to retrieve the SSL parameters from the selected device.
 - ii. From the **Select Server SSL Profile** dropdown, select the required client SSL profile.
 - c. **None:** If this option is selected, no client SSL profiles will be associated to the VIP.
15. From the **HTTP Profile** dropdown, select one of the following options and complete the corresponding steps:
 - a. **Create New HTTP Profile**
 - i. Click the **Fetch HTTP Profiles** button to retrieve the HTTP profiles from the selected device.
 - ii. In the **HTTP Profile Name** box, provide a name for the HTTP profile or click the  (**Retrieve field values**) button to search for and select the existing HTTP profile.
 - b. **Use Existing HTTP Profile**
 - i. Click the **Fetch HTTP Profiles** to retrieve the HTTP profiles from the selected device.
 - ii. From the **Select HTTP Profile** dropdown, select the required HTTP profile.
 - c. **None:** If this option is selected, no client HTTP profiles will get associated to the VIP.
16. From the **Persistence** dropdown, select one of the following options and complete the corresponding steps:
 - a. **Create New Persistence**
 - i. From the **Persistence Type** dropdown, select the required type of persistence profile.
 - ii. In the **Persistence Profile Name** box, provide a name for the persistence profile.
 - b. **Use Existing Persistence**
 - i. Click the **Fetch Persistence Profiles** to retrieve the persistence profiles in the selected device.
 - ii. From the **Select Persistence** dropdown, select the required persistence.
 - c. **None:** If this option is selected, no client Persistence profiles will be associated to the VIP.
17. From the **SNAT** dropdown, select one of the following options and complete the corresponding steps:


a. SNAT Pool

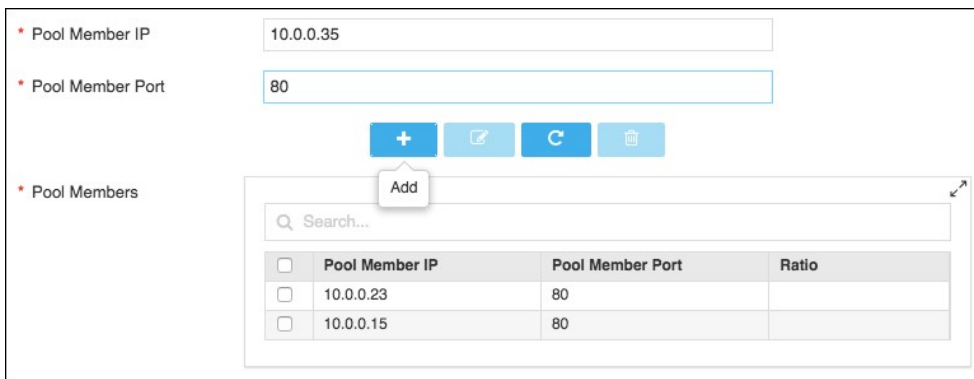
- i. In the **SNAT Pool Name** box, provide a name for the SNAT or click  (**Retrieve field values**) to search for and select the existing SNAT.
 - ii. In the **SNAT IP** box, provide the IP address of the SNAT.
 - iii. (Optional) In the Comments box, add additional information.
 - iv. Add pool members to the table by specifying the **SNAT Pool IP** and **Pool Member Port** and clicking the  (**Add**) button. Add all pool members who should be associated with the created virtual server.
- b. **automap**: Selecting this option will associate SNAT to the virtual server automatically.
 - c. **None**: If this option is selected, no SNAT will be associated to the VIP.
18. From the **Create Monitor?** dropdown, select one of the following options and complete the corresponding steps:

a. Yes

- i. From the Monitor Type dropdown, select **http**, **https**, or **tcp** monitor.
- ii. **Internal (seconds)** – The frequency at which the monitor will check the health of HTTP service on a pool
- iii. **Timeout (seconds)** – Specify the time to wait for an expected response, before changing the status of pool as down.
- iv. **Send String** – Query string sent as part of http client request.
- v. **Receive String** – Response string expected as part of http server response.

b. No

19. From the **Select Existing Monitors** dropdown, select the required monitor.
20. Select the load-balancing algorithm from the **Load Balancing Method** dropdown list.
21. Add pool members to the table by specifying the **Pool Member IP** and **Pool Member Port** and clicking the  (**Add**) button. Add all pool members who should be associated with the created virtual server.



* Pool Member IP: 10.0.0.35

* Pool Member Port: 80

+ edit refresh trash

* Pool Members

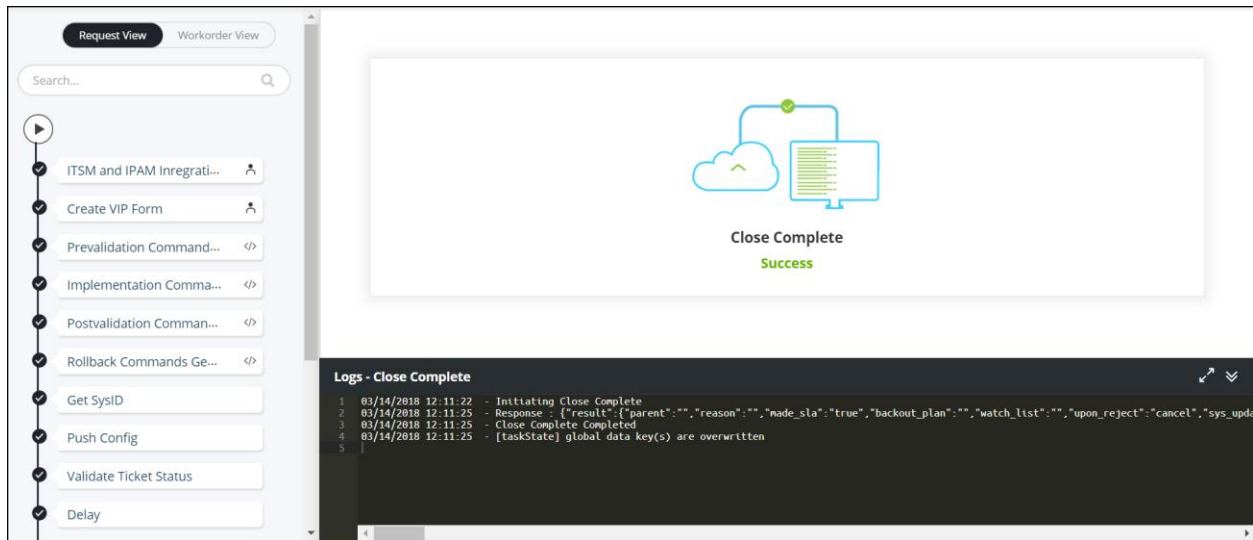
Search...

<input type="checkbox"/>	Pool Member IP	Pool Member Port	Ratio
<input type="checkbox"/>	10.0.0.23	80	
<input type="checkbox"/>	10.0.0.15	80	

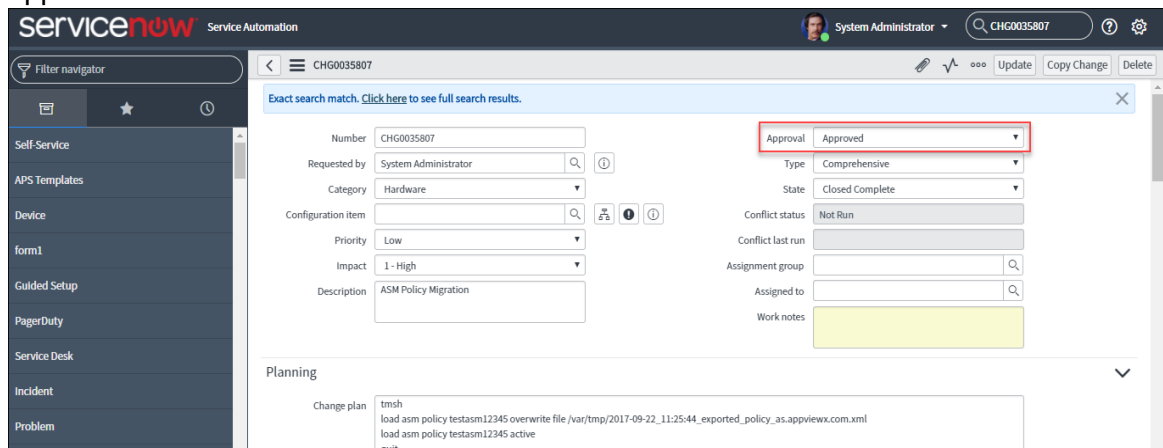
Workorder Flow

The following are the workorder tasks of *Create a Virtual Server* 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. **ITSM and IPAM Integration** — ITSM and IPAM is integrated with the use case that is being created.
2. **Create VIP Form** — Get the VIP creation details from the user.
3. **Prevalidation Command Generation** — The pre-validation commands are generated to initiate the pre-validation process.
4. **Implementation Command Generation** — The configuration commands are generated to implement the creation of a virtual server from a source device.
5. **Rollback Command Generation** — The configuration commands are generated to roll back the virtual server and LTM objects of the source device.
6. **Get SysID** — The Sys-ID for the *Create Virtual Server* workflow is generated to track the ServiceNow request.
7. **Push Config** — The generated configuration is pushed to the service now ticket.
8. **Validate Ticket Status** — To validate the ticket, log in to ServiceNow and manually approve the ticket.



9. **Approval** — Approval 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. Configuration changes are implemented on the device only after approval is received.

10. **Validate Ticket Status** — To validate the ticket, log in to ServiceNow and manually approve the ticket.
11. **Prevalidation** — Check the following:
 - A list of virtual servers available in the source and destination device.
 - The performance metrics, such as CPU and memory utilization on the destination device, have been validated.
12. **Implementation** — The configuration commands are implemented, resulting in the creation of a virtual server from a source device.
13. **Post-Validation** — Checks to see if the virtual server has been created successfully.
14. **Close** — After successful creation of the virtual server, the status of the ServiceNow ticket is updated automatically.

ServiceNow Service Automation

System Administrator CHG0035807

Filter navigator

Self-Service

APS Templates

Device

form1

Guided Setup

PagerDuty

Service Desk

Incident

Problem

CHG0035807

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.appvieww.com.xml
load asm policy testasm12345 active
quit
```

Rollback

The following are the workorder tasks of *Create a Virtual Server* 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.

Request View Workorder View

Search...

Rollback Approval 1

Prevalidation

Rollback

Postvalidation

DNS_Rollback

DNS_Rollback Success

Logs - DNS_Rollback

```
1 03/14/2018 12:14:33 - Initiating DNS_Rollback
2 03/14/2018 12:14:40 - IP Unreserved - DNS record(s) deleted
3 03/14/2018 12:14:43 - DNS_Rollback Completed
4 03/14/2018 12:14:43 - [taskState] global data key(s) are overwritten
```

1. **Rollback 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. Configuration changes are implemented on the device only after approval is received.

2. **Prevalidation** — Check the following:
 - The virtual servers is available on the selected device.
 - The performance metrics, such as CPU and memory utilization on the destination device have been validated.
3. **RollBack** — The configuration commands are rolled back resulting in the deleting of a virtual server and new LTM object is created from a source device.
4. **Post-Validation** — Checks if the virtual server has been deleted successfully.


Request Inventory

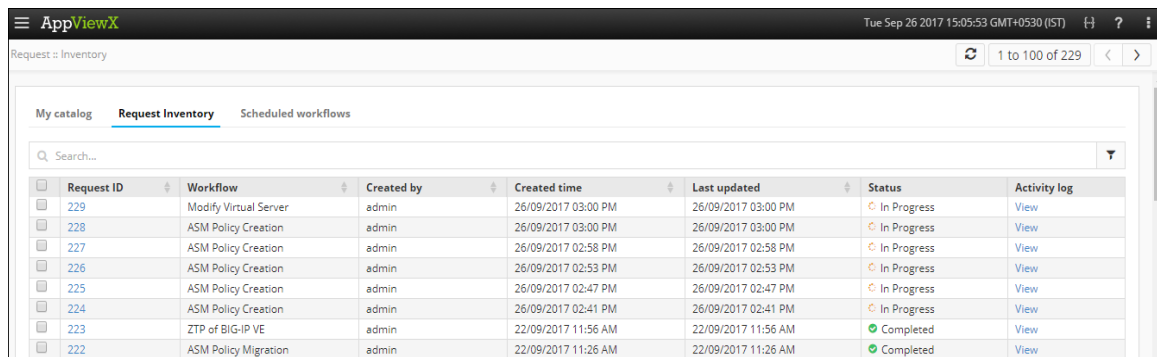
To go to the Request inventory, complete the following steps:

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.

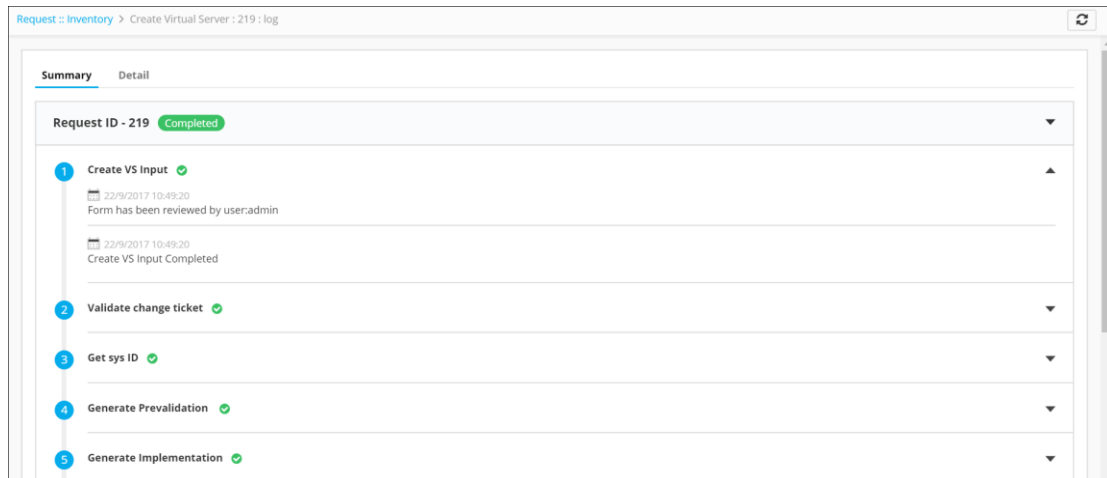
This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request using the **Search** field and/or click the  (**Filter**) button to select the options you want to use to sort the requests.



The screenshot shows the AppViewX interface with the 'Request Inventory' tab selected. It displays a table with the following data:



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** 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.






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**.

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.

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.