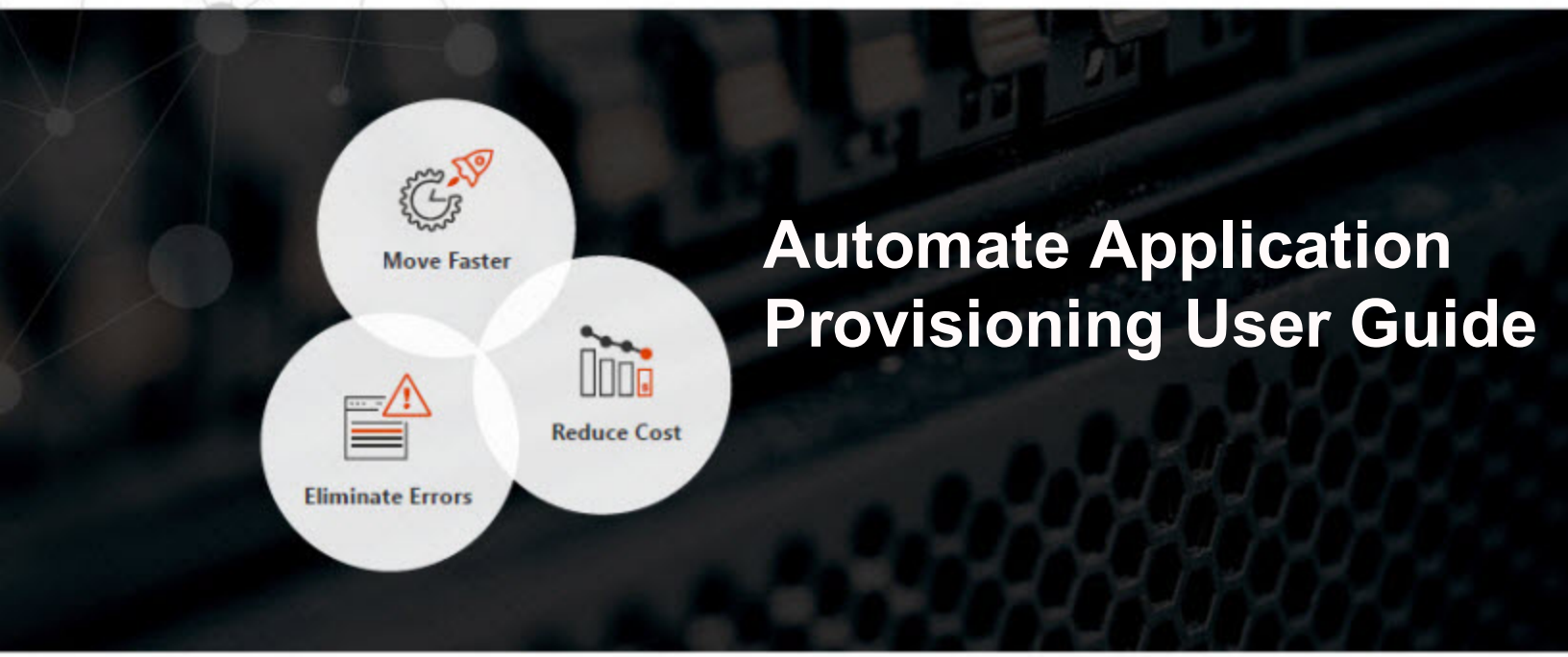
AppViewX



Automate Application Provisioning User Guide

Contact Information

AppViewX, Inc.

500 Yale Avenue North, Suite 100

Seattle, WA 98109

Tel: +1 (212) 400 7541

Tel: +44 (0) 203-514-2226

Email: info@appviewx.com

Web: http://www.appviewx.com

Document Version: 15062017_2035

Contents

Chapter 1: 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 roll-back. To get started, you can download Free AppViewX, which comes with a series of preloaded automation templates.

Chapter 2: AppViewX Automation Templates

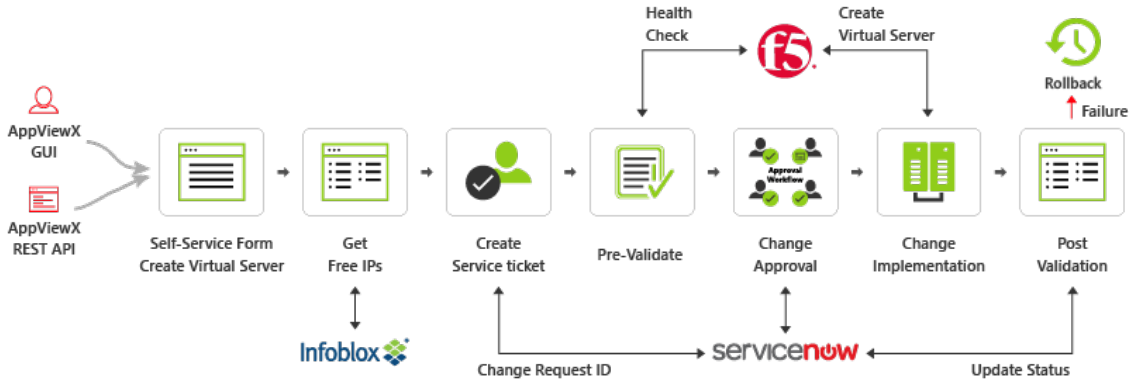
AppViewX comes with three automation templates to help you get started:

- Create Virtual Server
- Modify Virtual Server
- Delete Virtual Server

Each of these is discussed in detail in the sections below.

Create Virtual Server Template

The *Create Virtual Server* automation template 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 template filters F5 ADC devices based on the user's access permissions, defined by Role Based Access Control (RBAC). The platform integrates with 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 template 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.

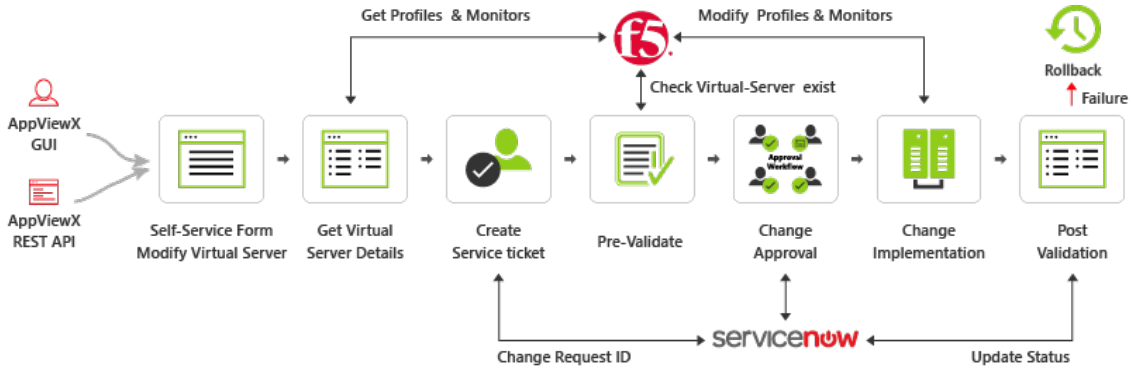


The work order pre-validates ADC device performance metrics (CPU and memory utilization) and confirms that the new virtual server and associated objects are not present. On successful pre-validation, the configuration changes are reviewed through a two-level approval process: first by ServiceNow, then 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. In case of failure, all changes implemented within the work order can be rolled back easily.

Modify Virtual Server Template

With the *Modify Virtual Server* automation template, users can add or delete iRules, profiles, monitors, and pool members on an existing virtual server. Like the Create Virtual Server template, this template filters F5 ADC devices based on the user's access permissions, defined by Role Based

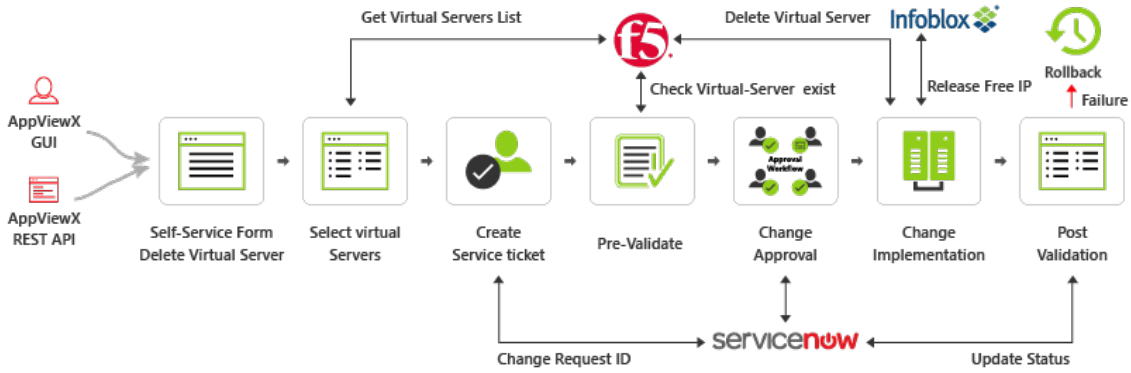
Access Control (RBAC), and displays the list of virtual servers available on the selected ADC device. When a virtual server is selected, object details like iRules, profiles, monitors, and pool members are displayed in the template fields. The template also provides an option to modify the association of these virtual server objects 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 a work order and is updated based on the implementation status.



The work order that is generated confirms the existence of the virtual server and its associated objects before any changes are made. 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 modified successfully. In case of failure, all changes implemented within the work order can be rolled back easily.

Delete Virtual Server Template

Multiple virtual servers and the associated objects like profiles and monitors can be deleted using the *Delete Virtual Server* automation template. Like the Create and Modify templates, this template filters available F5 ADC devices based on a user's access permissions, defined by Role Based Access Control (RBAC), and displays the list of virtual servers available on the selected ADC device. It provides an option to release the virtual server IP address and delete the DNS records in a IPAM system, such as Infoblox. The template can also integrate with ITSM systems such as ServiceNow for approvals and governance. When the form is submitted, a change request is created and the service request change ID is associated with the work order. This is updated based on the implementation status.



The first step in the work order is a pre-validation check to see if the virtual server exists. If the server does exist, the configurations needed to delete the virtual server and its associated profiles and monitors are reviewed through a two-level approval process: first by ServiceNow and then by AppViewX. After approval is granted, the virtual server and its unused dependent objects, like profiles and monitors, are deleted. A series of post-validation scripts ensure that the virtual server is deleted and any orphan objects are removed. In case of failure, all changes implemented within the work order can be rolled back easily.

Chapter 3: Prerequisites

To run the application provisioning automation templates in your environment, the following pre-requisites must be met:

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

Chapter 4: Compatible Software Versions

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

- AppViewX – Free AppViewX version and AVX 11.4.3
- ServiceNow – Geneva version
- Infoblox – version 7.2.X
- F5 LTM – version 10.X, 11.X, or 12.X

Chapter 5: 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`/`admin`.

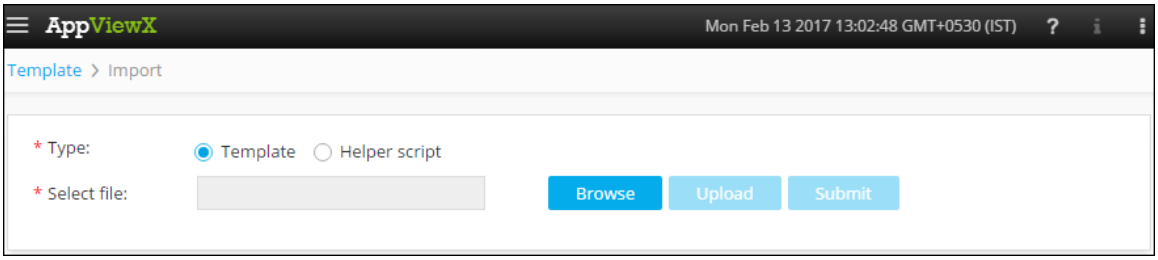
Note: It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

Import Templates and Helper Scripts

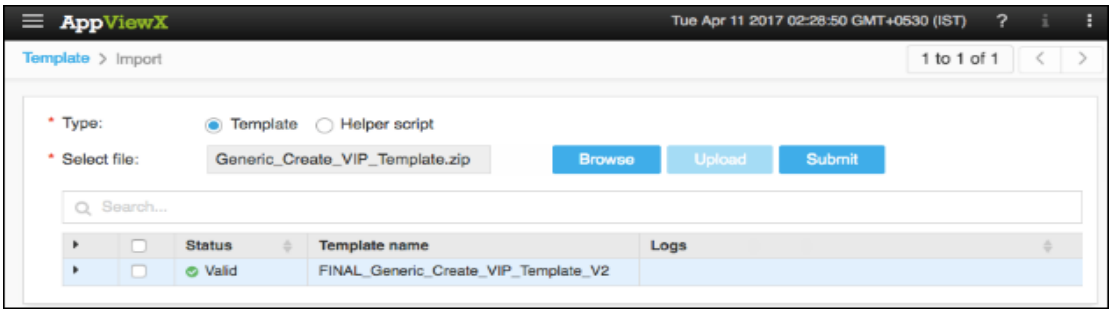
Note: Free AppViewX comes preloaded with application provisioning automation templates and helper scripts. You will only need to use the following import instructions when newer versions of the templates and helper scripts become available.

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Templates**.
2. Click the  (**Import**) button in the Command bar in the top-right corner of the screen.

   The following screen appears.



3. To import a template, complete the following sub-steps
   a. Select the **Template** radio button.
   b. Click **Browse**.
   c. Select the template file you want to import.
   d. Click **Upload** to import the file and view its contents.



e. In the table at the bottom of the Import page, select the check box beside the unzipped template file.

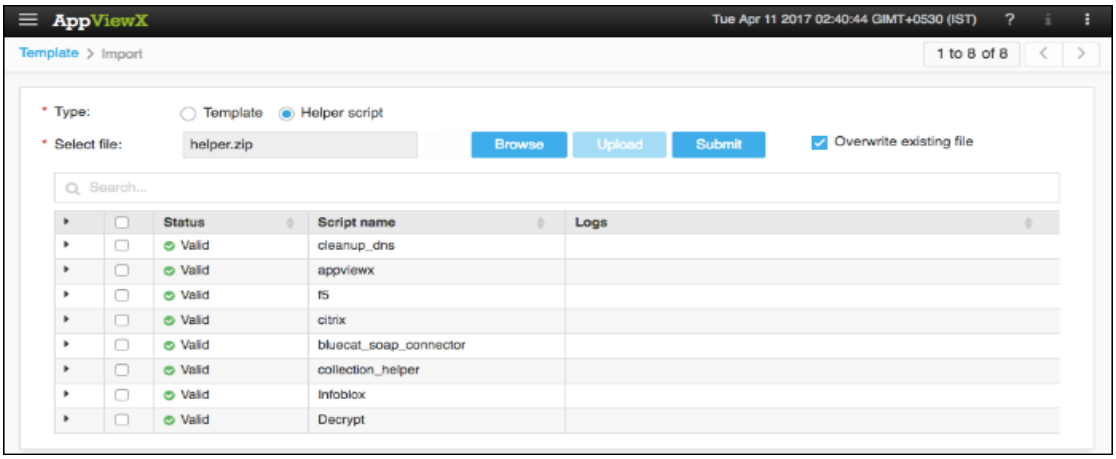
f. Click **Submit** to deploy the templates into your AppViewX environment.

4. To import a helper script, complete the following sub-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.

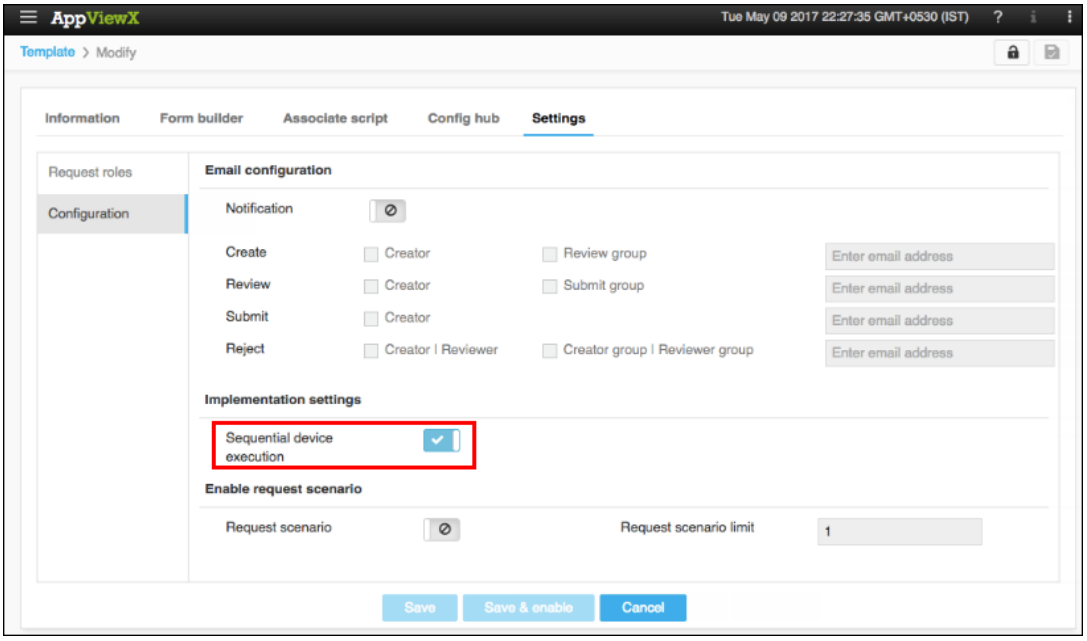
e. Click **Submit** to deploy them into your AppViewX environment.

5. Navigate to **Provisioning > Template**.

   The newly imported templates are disabled by default.

6. Select the check box beside the template name, then click the  (**Enable**) button in the Command bar.

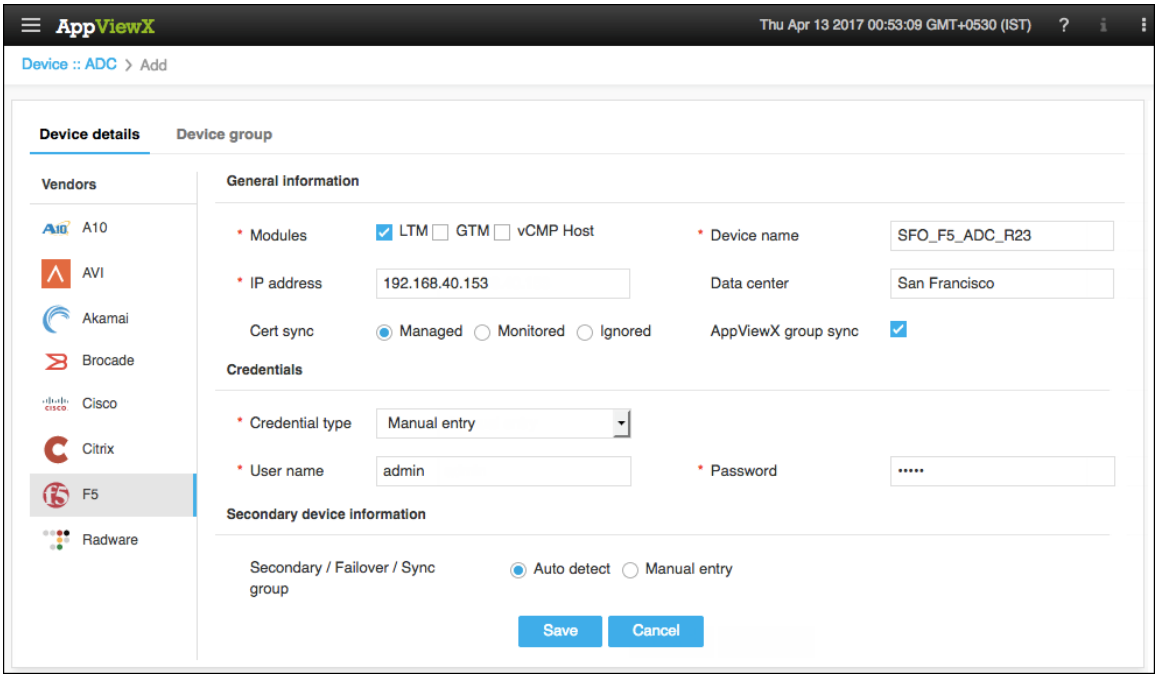
7. Navigate to **Template > Settings > Configuration** and select the **Sequential device execution** check box.



8. Click the **Save & enable** button.

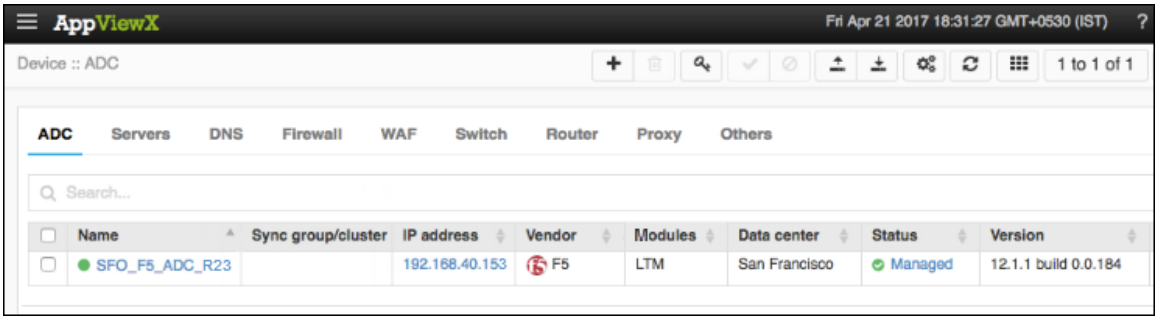
Add an ADC Device: F5 LTM

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.



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 drop-down menu.
12. 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.
13. Select **Auto detect** to automatically detect and add secondary or failover devices or sync groups to the ADC device inventory.
14. Click **Save** to save the new ADC device on the ADC tab.

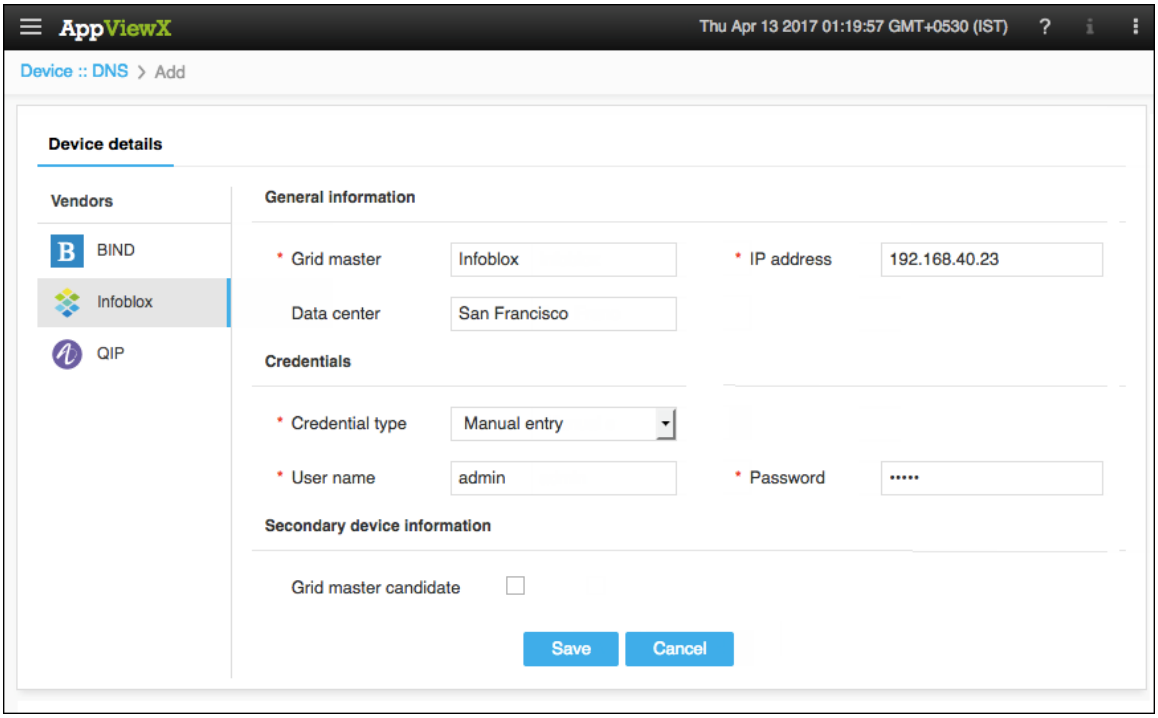


The device will display one of the following statuses:

- **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.

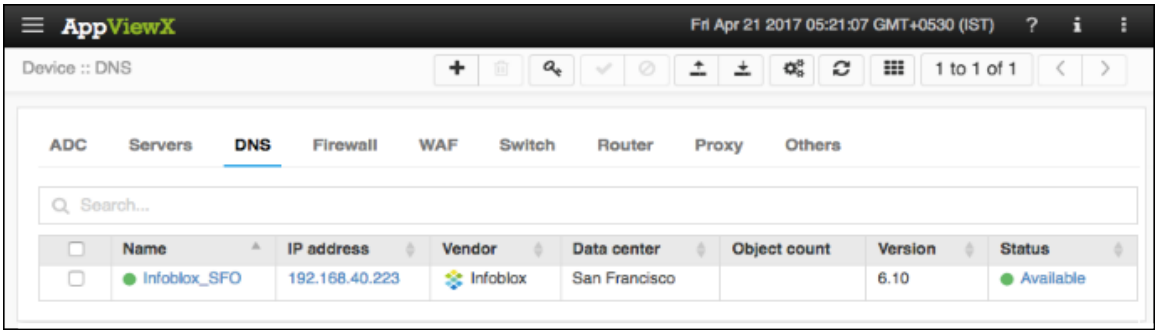
Add an IPAM Device: Infoblox

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.



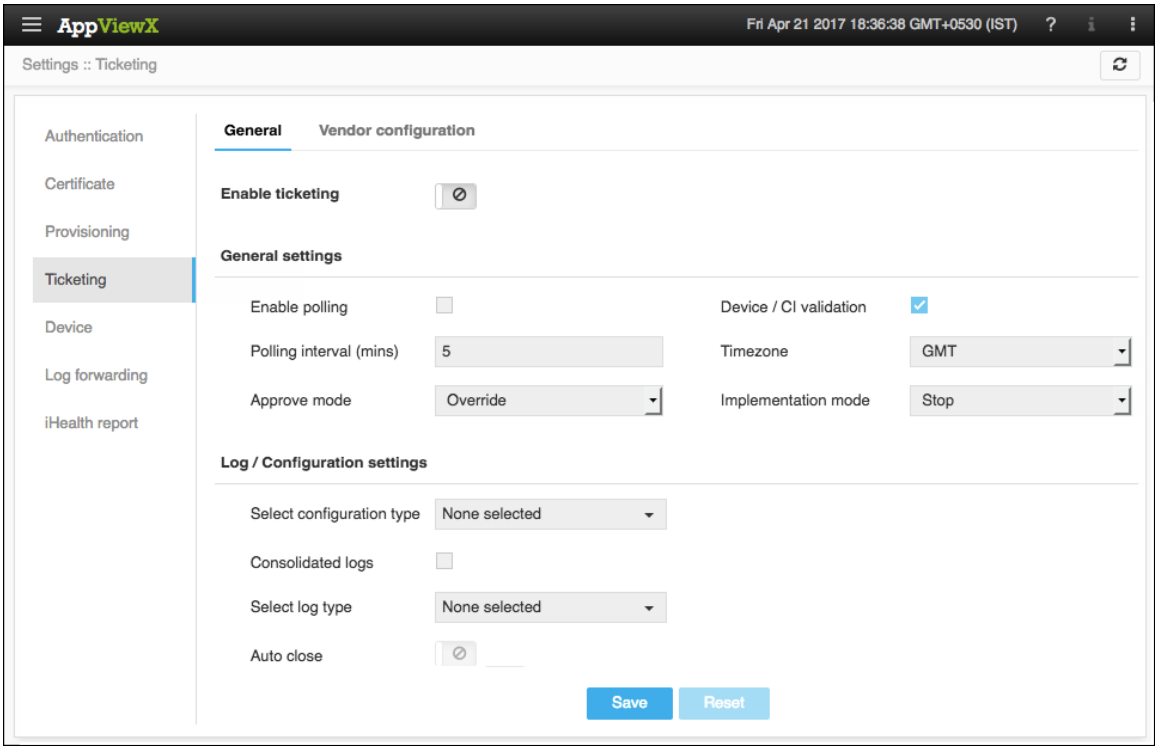
5. Click the **Save** button.

   The device status on the DNS tab changes to **Available** to indicate the successful addition of Infoblox.

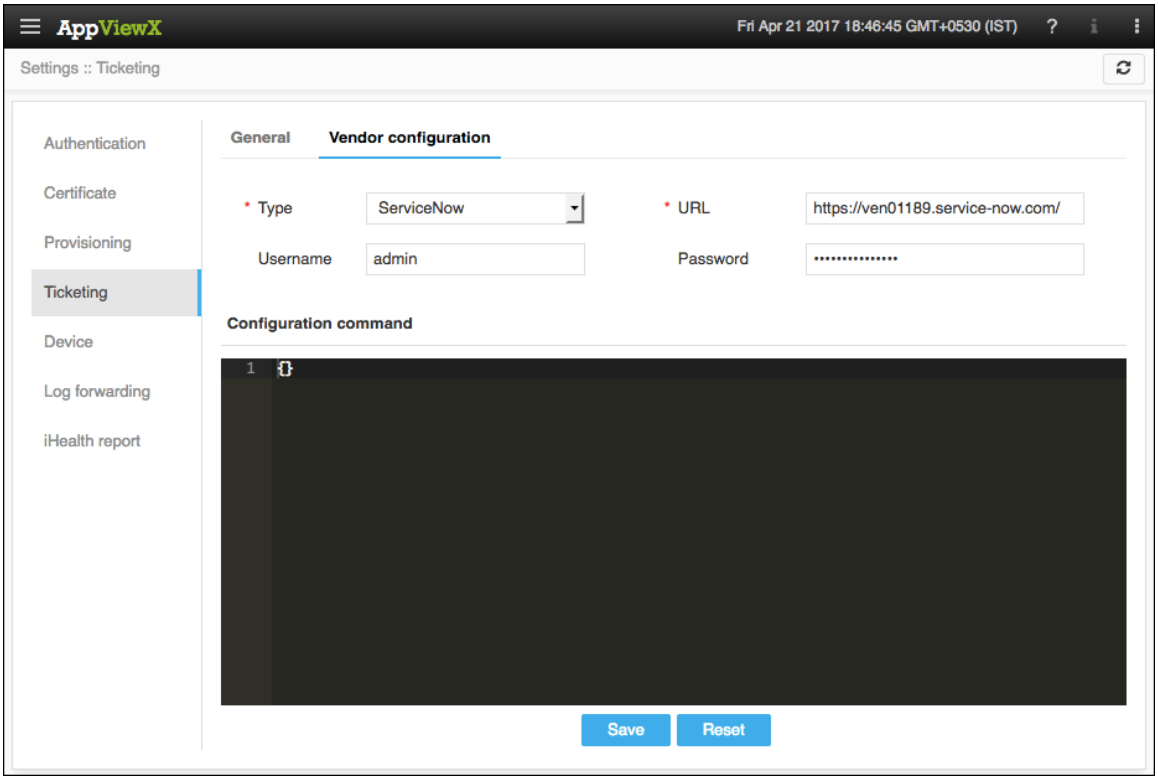


Register an ITSM Device: ServiceNow

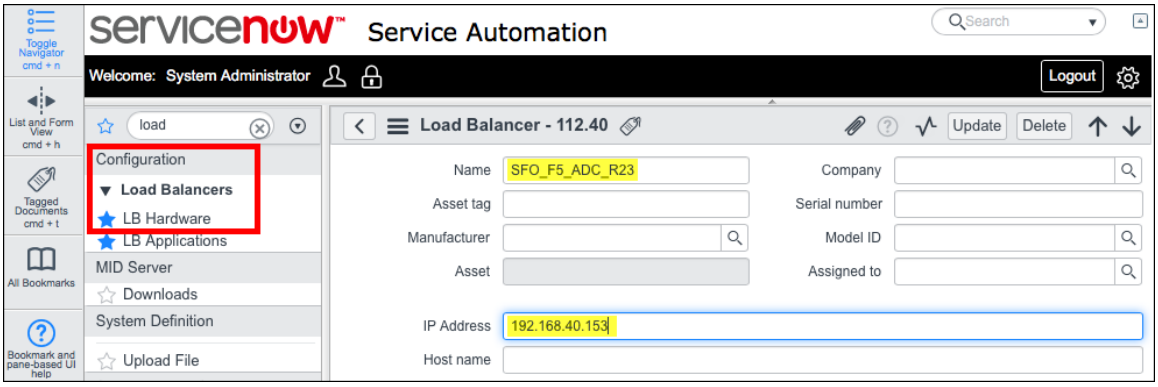
1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Settings**.
2. On the Settings page that opens, click **Ticketing** in the column on the left.



3. Click the **General** tab, then click to select **Enable ticketing**.
4. Click **Save**.
5. On the **Vendor configuration** tab, choose **ServiceNow** from the **Type** drop-down menu, then enter the ServiceNow web URL and credentials.



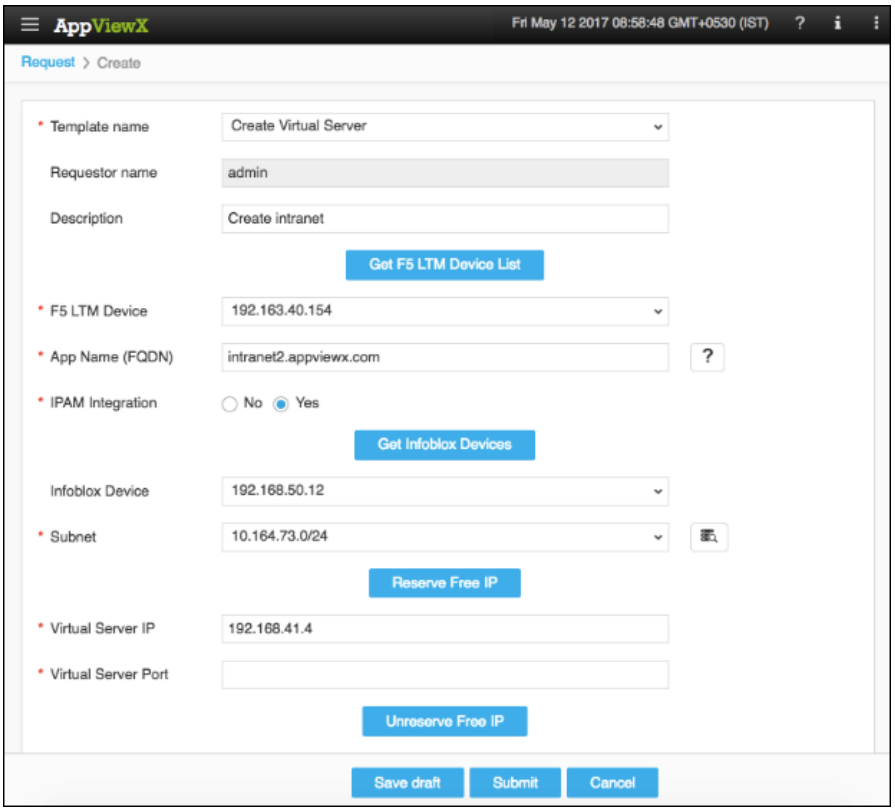
6. Click the **Save** button.
7. The F5 LTM device you are configuring should be present in the ServiceNow LB Hardware inventory. You can check this by opening ServiceNow and clicking to open the Load Balancers > LB Hardware section shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.



Create a Virtual Server

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Request**.
2. Click the + (**Add**) button in the Command bar.
3. Choose the **Create_Virtual_Server** template in the **Template Name** drop-down list.

Note: If the template is not available it is either not enabled or the import failed. Check the template status under **Provisioning > Template**.



4. Enter a **description** for the provisioning request.
5. Click the **Get F5 LTM Device List** button to fetch the list of managed F5 LTM devices.
6. In the **F5 LTM Device** field, select the device on which the virtual server is to be created.
7. Enter a valid virtual server name in the **App 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.

8. If **IPAM integration** is required, select the **Yes** radio button. The self-service form fields are updated automatically based on the selection.

   a. Click the **Get Infoblox Devices** button to fetch the available list of Infoblox devices.

   b. Select the **Infoblox Device** from the drop-down list, which will assign the free IP address.

   c. Retrieve the list of subnets available on the selected Infoblox device by clicking the  (**Fetch**) button and selecting the required subnet.

   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 addresses on Infoblox.

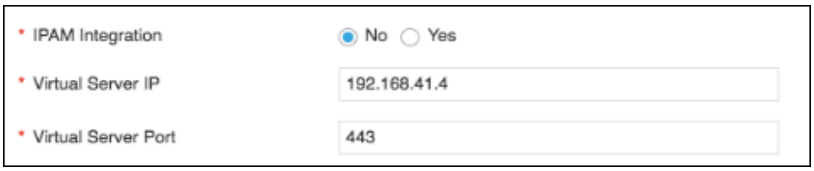
e. If the IP address is reserved from an incorrect subnet , click the **Unreserve Free IP** button to delete the DNS binding and release the IP address in Infoblox.

f. Enter the **Virtual Server Port** number used to access the application.

If IPAM integration is not required, select **No**.

a. Enter a virtual server IP in the **Virtual Server IP** field.

b. Enter a virtual server port in the **Virtual Server Port** field.

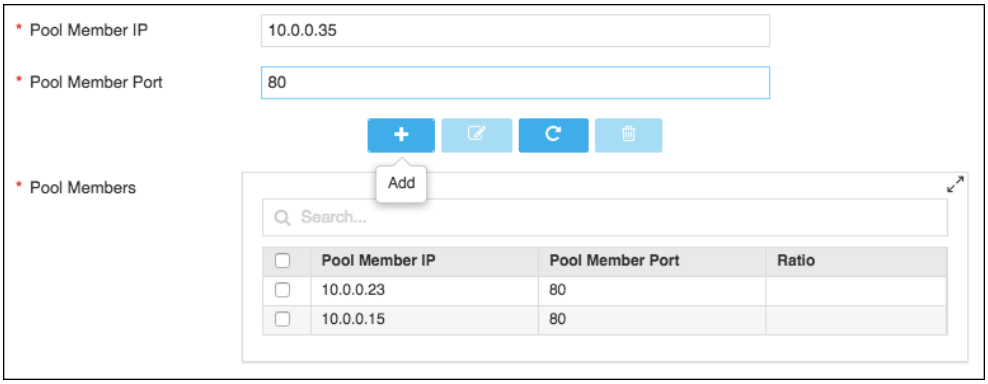


9. Click the **Get LTM Device Details** button to retrieve virtual server related details from the selected device and populate the form fields, like profiles and monitors.
10. Select **Persistence Profile** from the list of available profiles.
11. Select **Yes** in the **Associate HTTP Profile** field, then select **HTTP Profile** from the available drop-down list.
12. Select **Yes** in the **Create HTTP Monitor** field to associate it with the virtual server.
13. Create a new HTTP monitor with the following field settings:

- **Internal (seconds)** – The frequency at which the monitor will check the health of HTTP service on a pool
- **Timeout (seconds)** – Specify the time to wait for an expected response, before changing the status of pool as down.
- **Receive String** – Response string expected as part of http server response.
- **Send String** – Query string sent as part of http client request.

14. Select an existing monitor in the **Associate Existing Monitor** drop-down list to associate it with the created Virtual Server.
15. Select the load-balancing algorithm from the **Load Balancing Method** drop-down list.
16. 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

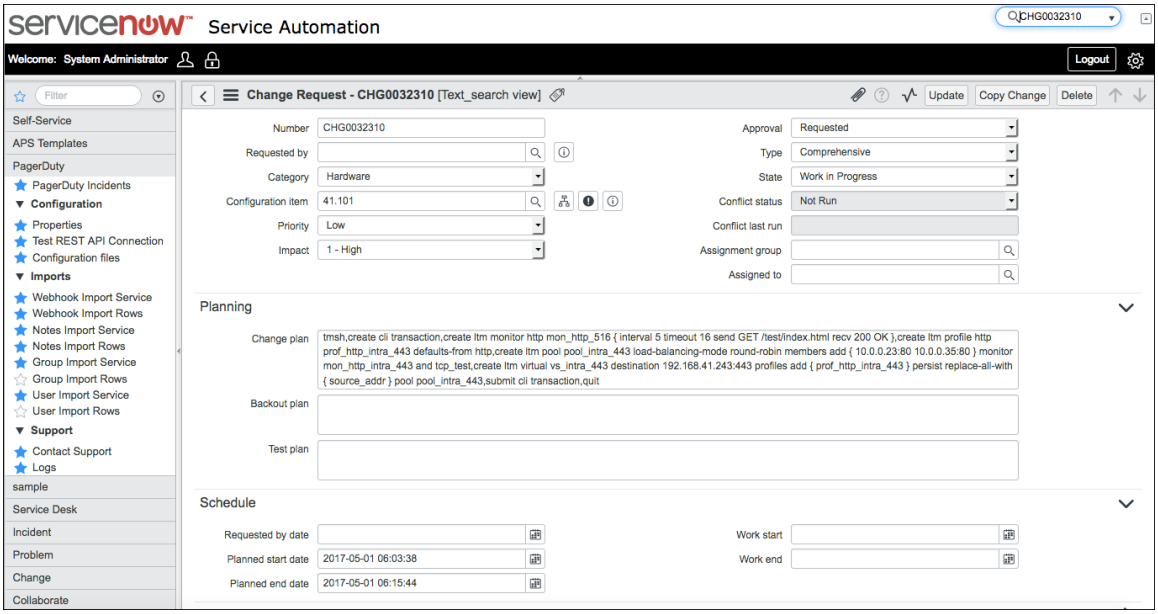
created virtual server.



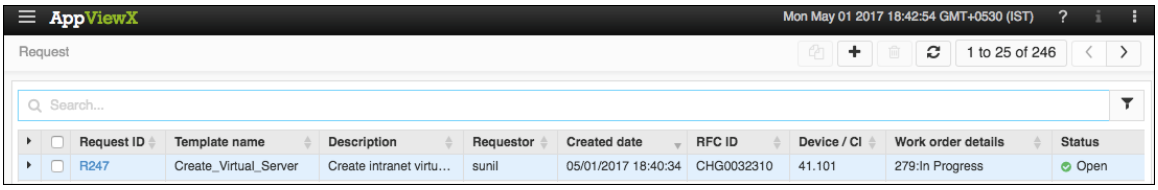
17. In the **ITSM Integration** field, select **Yes**. This creates a ServiceNow change request ticket and binds it with the work order to update the ServiceNow status.

18. Select the **Time Zone** of the F5 LTM device that you are configuring.
19. Schedule the maintenance window time and date using the **Planned Start Date** and **Planned End Date** fields. The configuration changes will be implemented during this maintenance window.
20. Click the **Create ServiceNow Request** button to create a new ServiceNow ticket and auto-populate the **Change Request ID** field.

    AppViewX then creates the ServiceNow change request and populates the change request fields like **Configuration item**, **Planned start date**, and **Planned end date** from the self-service form. The **Change plan** field is populated with the proposed F5 LTM configuration changes, which can be reviewed at any time by the approver.



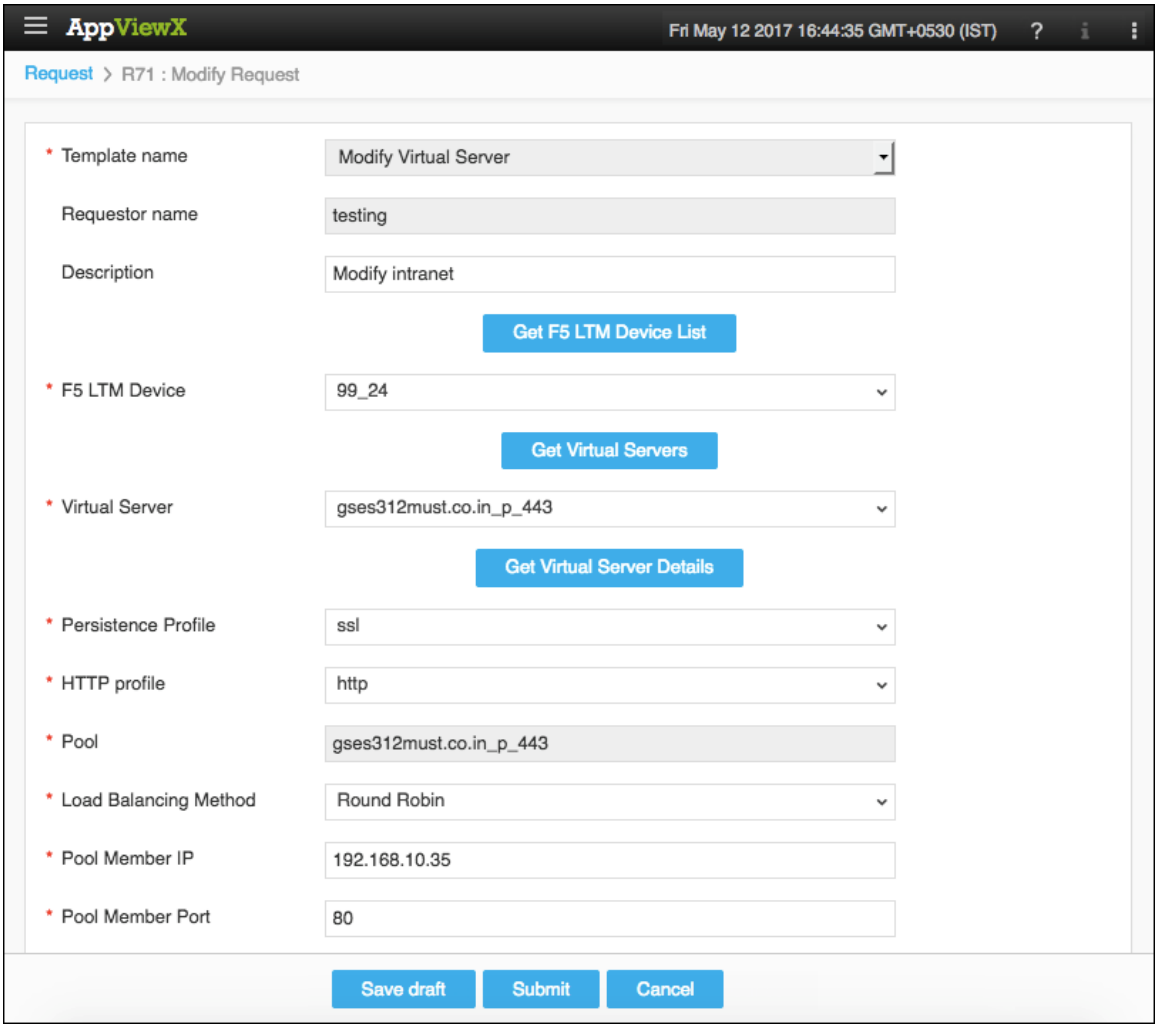
21. Click **Submit** to submit the self-service form and create the work order and associate it with the ServiceNow change request ID (RFC-ID) in the AppViewX system.



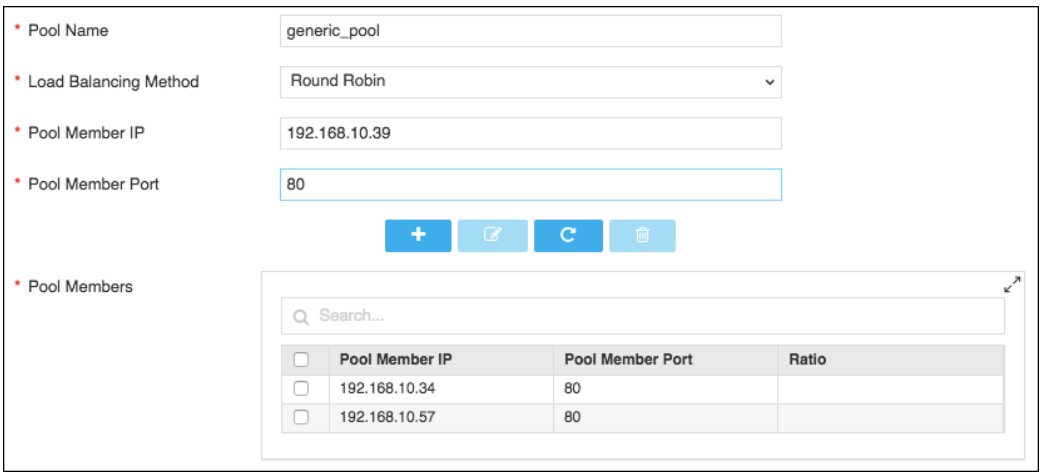
Modify a Virtual Server

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Request**.
2. Click the + (**Add**) button in the Command bar.
3. Select the **Modify Virtual Server** template from the **Template Name** drop-down list.

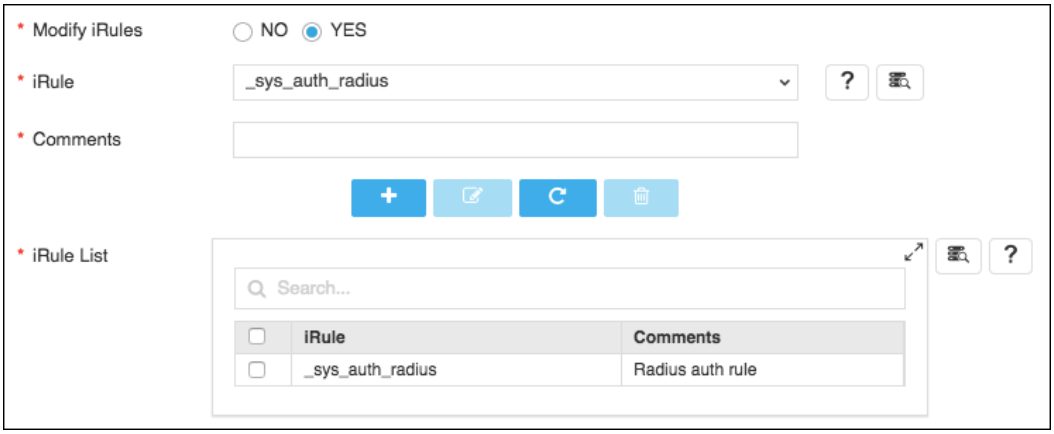
   Note: If the template is not available, it is either not enabled or the import failed. Check the template status by navigating to **Provisioning > Template**.



4. Enter a **description** for the provisioning request.
5. Click the **Get F5 LTM Device List** button to fetch the list of managed F5 LTM devices.
6. In the **F5 LTM Device** field, select the device that contains the virtual server that is to be modified.
7. Click the **Get Virtual Servers** button to fetch the list of virtual servers from the device.
8. Select a **Virtual Server** from the drop-down list.
9. Click the **Get Virtual Server Details** button to retrieve the virtual server configurations.
10. Select a **Persistence Profile** from the drop-down list.
11. Select an **HTTP Profile** from the drop-down list.
12. (Optional) Edit the **Pool Name** of the virtual server pool.



13. Select a **Load Balancing Method** for the pool members from the drop-down list.
    The Pool Members corresponding to the selected virtual server are displayed in the table.
    a. (Optional) Modify an existing pool member by selecting the check box beside its name and clicking the (**Modify**) button.
    b. (Optional) Delete an existing pool member by selecting the check box beside its name and clicking the (**Delete**) button.
    c. (Optional) Add a new pool member by filling in the Pool Member IP and Pool Member Port fields and clicking the (**Add**) button.
14. In the **Modify iRules** field, select the **YES** radio button.

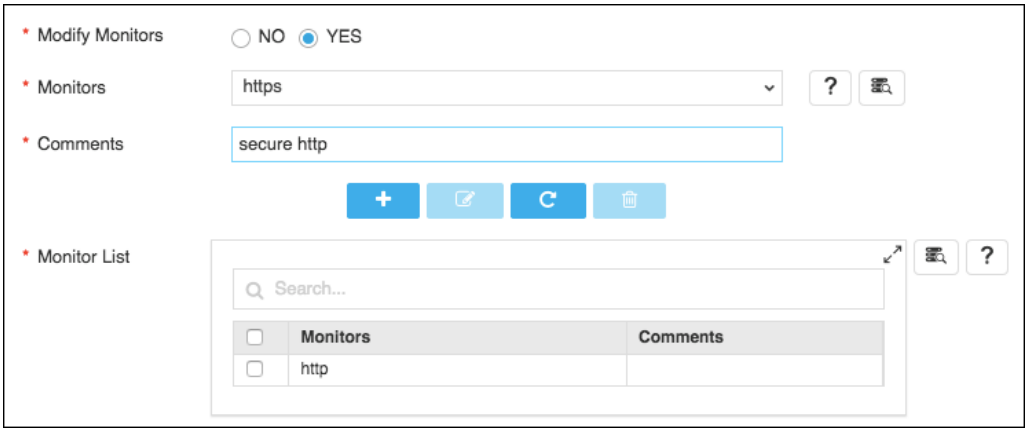


    a. Click the (**Fetch**) button at the right side of the **iRule** field to retrieve the list of available iRules for the selected F5 LTM device.
    b. In the **iRule** field, select an iRule from the drop-down list.
    c. In the **Comments** field, enter comments related to the iRule.
    d. Click the (**Add**) button to associate the iRule with the virtual server.

e. Click the  (**Fetch**) button under the iRule List field to retrieve the list of iRules already associated with the virtual server.

f. (Optional) Modify or delete iRules in the **iRule List** using the  (**Modify**) button or the  (**Delete**) button.

15. In the **Modify Monitors** field, select the **YES** radio button.



a. Click the  (**Fetch**) button at the right side of the **Monitors** field to retrieve available monitors for the selected F5 LTM device.

b. In the **Monitors** field, select a monitor from the drop-down list to associate it with virtual server.

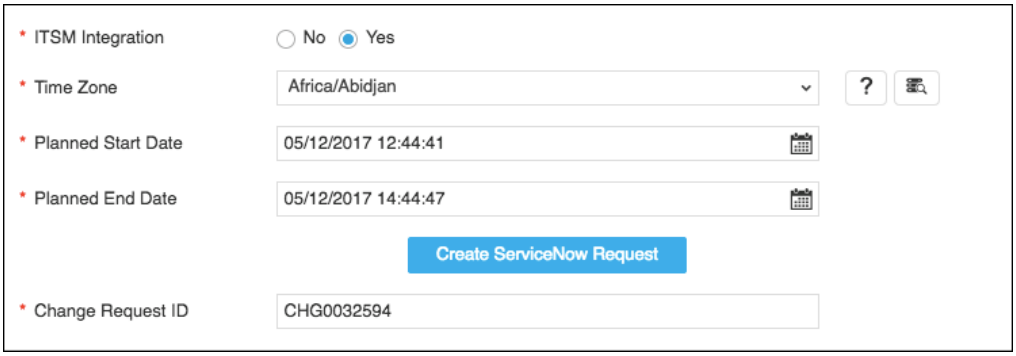
c. In the **Comments** field, enter comments related to the monitor.

d. Click the  (**Add**) button to associate the monitor with the virtual server.

e. Click the  (**Fetch**) button at the right side of the **Monitor List** field to retrieve the list of monitors already associated with the virtual server.

f. (Optional) Modify or delete monitors in the **Monitor List** using the  (**Modify**) button or the  (**Delete**) button.

16. In the **ITSM Integration** field, select the **Yes** radio button. This creates a ServiceNow change request ticket and binds it to the work order to update the ServiceNow status.

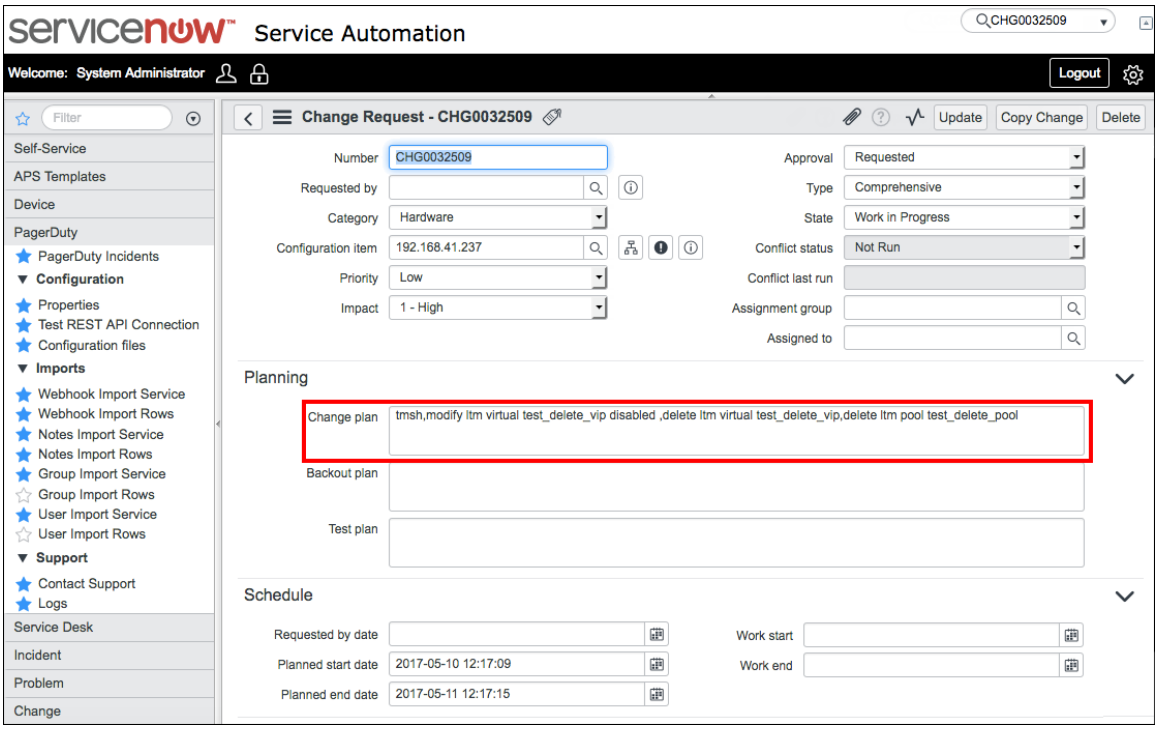


a. Select the **Time Zone** of the F5 LTM device that you are configuring.

b. Schedule the maintenance window time and date using the **Planned Start Date** and **Planned End Date** fields. The configuration changes will be implemented during this maintenance window.

c. Click the **Create ServiceNow Request** button to create a new ServiceNow ticket and auto-populate the **Change Request ID** field.

AppViewX then creates the ServiceNow change request and populates the change request fields like **Configuration item**, **Planned start date**, and **Planned end date** from the self-service form. The **Change plan** field is populated with the proposed F5 LTM configuration changes, which can be reviewed at any time by the approver.

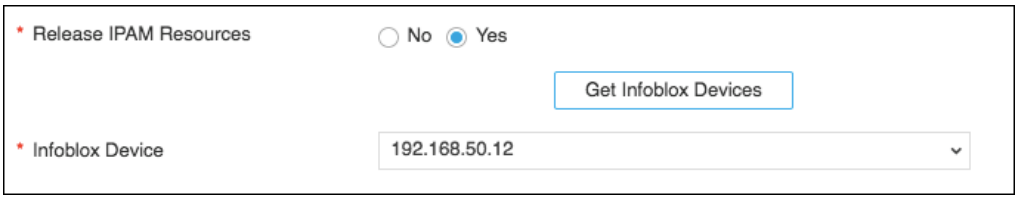


17. Click **Submit** to submit the self-service form and create the work order and associate it with the ServiceNow change request ID (RFC-ID) in the AppViewX system.

Delete a Virtual Server

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Request**.
2. Click the + (**Add**) button in the Command bar to create a new service request.
3. Select the **Delete Virtual Server** template from the **Template Name** drop-down list.

   Note: If the template is not available it is either not enabled or the import failed. Check the template status under **Provisioning > Template**.
4. Enter a **description** for the provisioning request.
5. Click the **Get F5 LTM Device List** button to fetch the list of managed F5 LTM devices.
6. In the **F5 LTM Device** field, select the device that contains the virtual server that you want to delete.
7. Click the **Get Virtual Servers** button to fetch the list of virtual servers on the device you selected in Step 6.
8. Select one or more virtual servers from the **Virtual Servers List** drop-down list.
9. In the **Release IPAM Resources** field, select the **Yes** radio button. This deletes the server's DNS records and releases the IP address assigned to the virtual server in Infoblox.



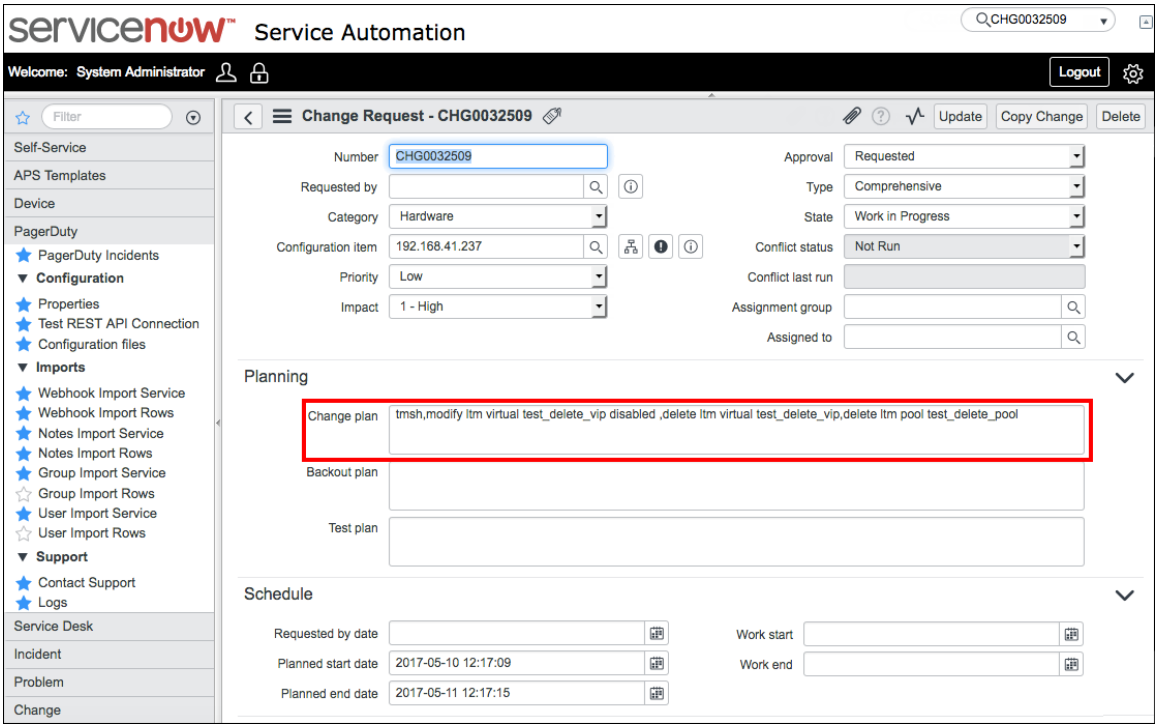
10. Click the **Get Infoblox Devices** button.
11. In the **Infoblox Device** field, select the Infoblox device that contains the DNS records you want to delete.
12. In the **ITSM Integration** field, select the **Yes** radio button. This creates a ServiceNow change request ticket and binds it to the work order to update the ServiceNow status.

   a. Select the **Time Zone** of the F5 LTM device that you are configuring.

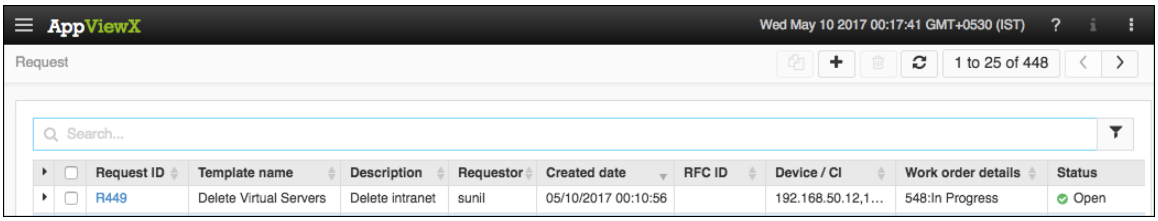
b. Schedule the maintenance window time and date using the **Planned Start Date** and **Planned End Date** fields. The configuration changes will be implemented during this maintenance window.

c. Click the **Create ServiceNow Request** button to create a new ServiceNow ticket and auto-populate the **Change Request ID** field.

AppViewX then creates the ServiceNow change request and populates the change request fields like **Configuration item**, **Planned start date**, and **Planned end date** from the self-service form. The **Change plan** field is populated with the proposed F5 LTM configuration changes, which can be reviewed at any time by the approver.

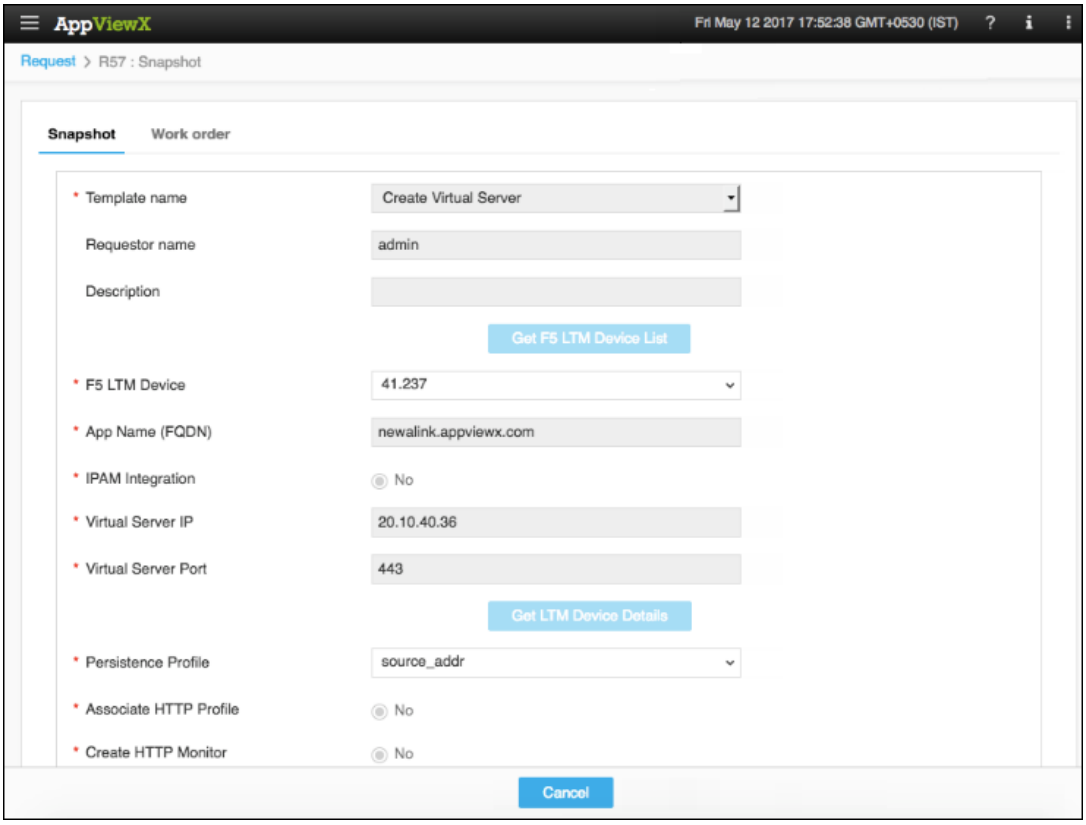


13. Click **Submit** to submit the self-service form and create the work order and associate it with the ServiceNow change request ID (RFC-ID) in the AppViewX system.

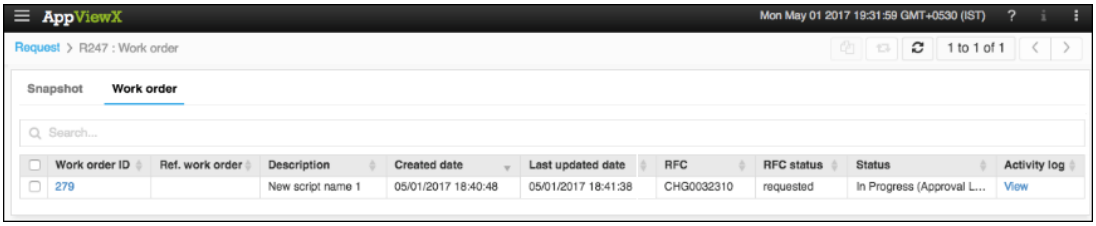


Review and Approve

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Request**.
2. Locate the submitted request you want to review, then click the **Request ID** number to view a snapshot it.

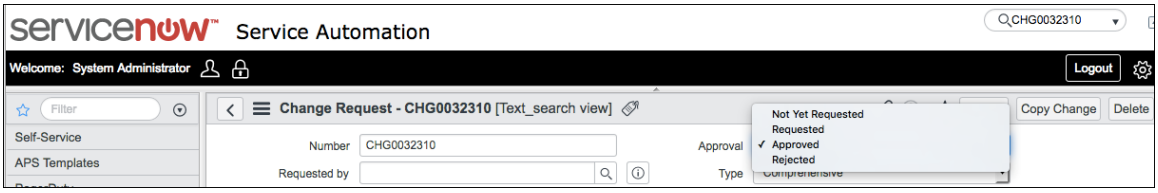


3. Click the **Work Order** tab to view the work order details and status for the request.



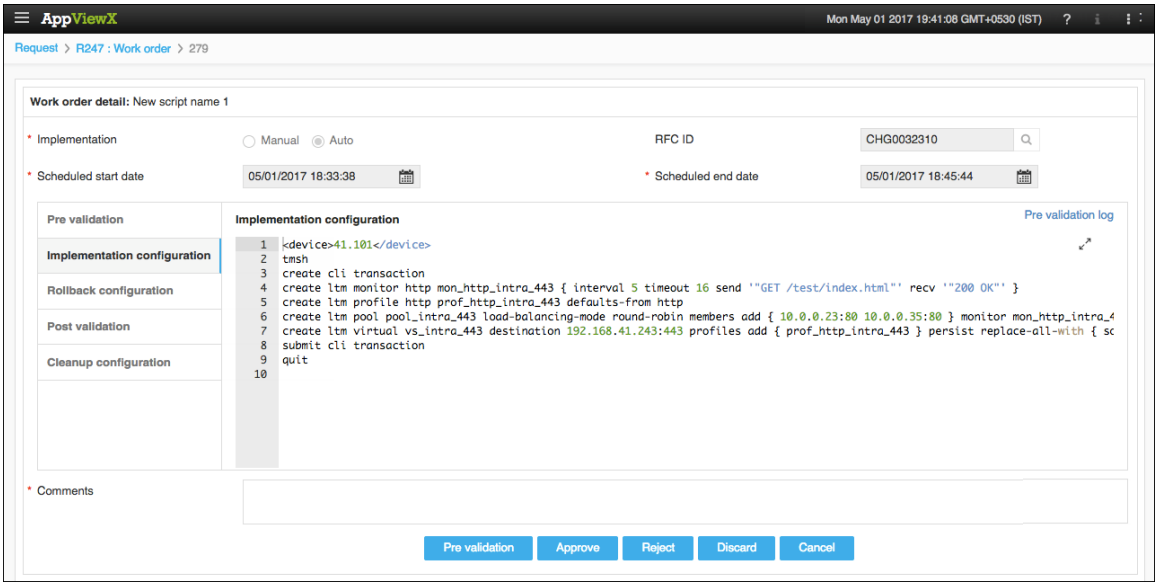
Note: The current version requires a single-level approval at both ServiceNow and AppViewX. However AppViewX workflow provides the flexibility to customize single-level or multi-level approvals either at ServiceNow or AppViewX only.

4. If the RFC status of the work order is "*requested*," as it is for the request in the image above, approve the change request in ServiceNow first by clicking the **Approval** field and selecting **Approved** from the drop-down list.

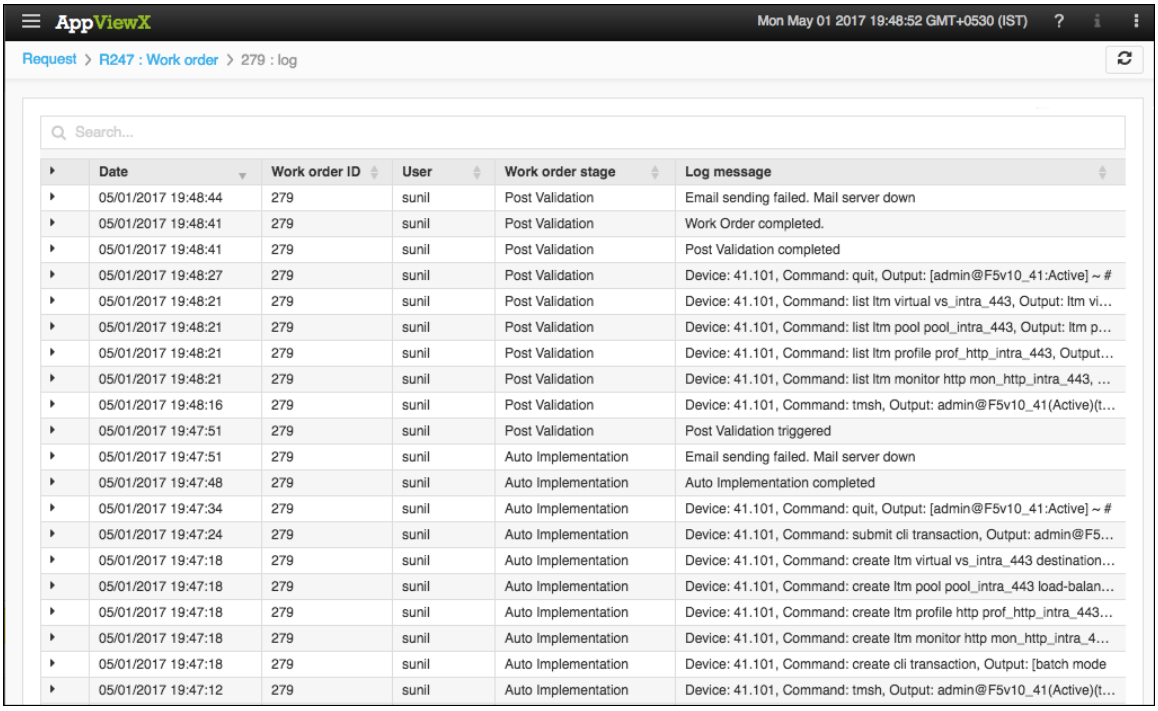


Back in AppViewX, the work order **RFC status** column changes to **Approved**.

5. Click the link in the **Work order ID** column to open the work order details screen
6. Click the **Implementation configuration** tab and review the configuration details.

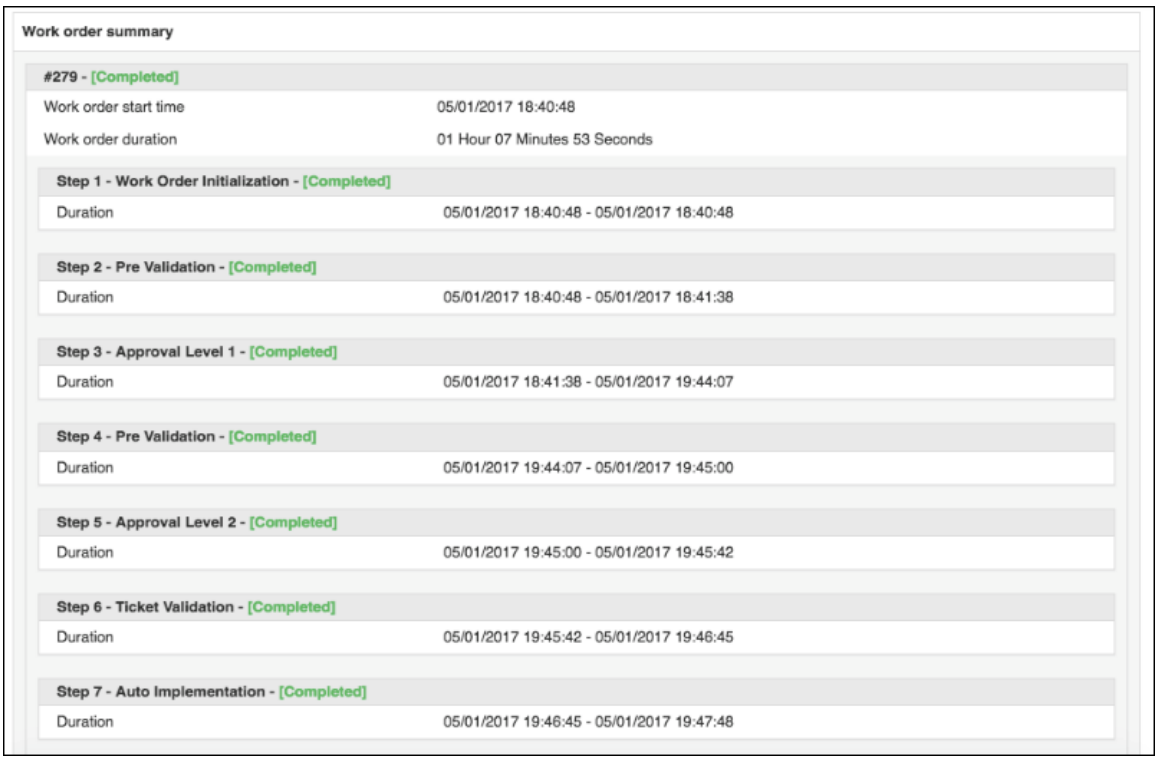


7. In the **Comments** field, enter details about the implementation configuration.
8. Approve the work order by clicking the **Approve** button.
9. Back on the *Work order details* screen, click the **View** link in the **Activity log** column to check the work order logs, which provide useful information for understanding the work order flow and for troubleshooting.

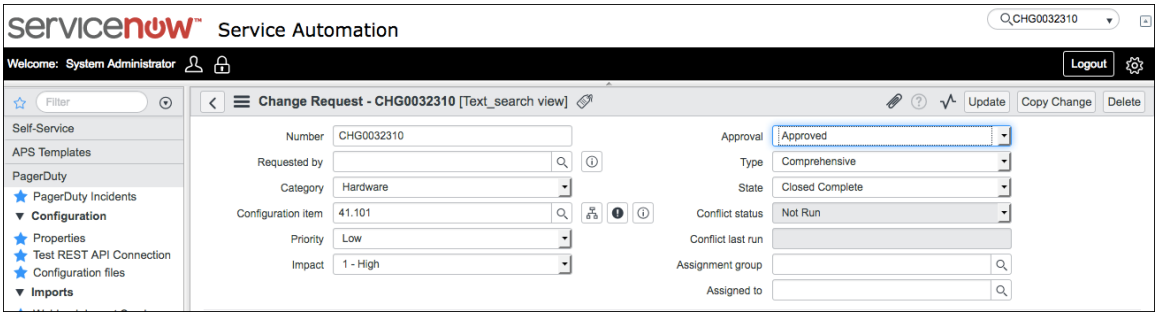


Date	Work order ID	User	Work order stage	Log message
05/01/2017 19:48:44	279	sunil	Post Validation	Email sending failed. Mail server down
05/01/2017 19:48:41	279	sunil	Post Validation	Work Order completed.
05/01/2017 19:48:41	279	sunil	Post Validation	Post Validation completed
05/01/2017 19:48:27	279	sunil	Post Validation	Device: 41.101, Command: quit, Output: [admin@F5v10_41:Active] ~ #
05/01/2017 19:48:21	279	sunil	Post Validation	Device: 41.101, Command: list ltm virtual vs_intra_443, Output: ltm vi…
05/01/2017 19:48:21	279	sunil	Post Validation	Device: 41.101, Command: list ltm pool pool_intra_443, Output: ltm p…
05/01/2017 19:48:21	279	sunil	Post Validation	Device: 41.101, Command: list ltm profile prof_http_intra_443, Output…
05/01/2017 19:48:21	279	sunil	Post Validation	Device: 41.101, Command: list ltm monitor http mon_http_intra_443, …
05/01/2017 19:48:16	279	sunil	Post Validation	Device: 41.101, Command: tmsh, Output: admin@F5v10_41(Active)(t…
05/01/2017 19:47:51	279	sunil	Post Validation	Post Validation triggered
05/01/2017 19:47:51	279	sunil	Auto Implementation	Email sending failed. Mail server down
05/01/2017 19:47:48	279	sunil	Auto Implementation	Auto Implementation completed
05/01/2017 19:47:34	279	sunil	Auto Implementation	Device: 41.101, Command: quit, Output: [admin@F5v10_41:Active] ~ #
05/01/2017 19:47:24	279	sunil	Auto Implementation	Device: 41.101, Command: submit cli transaction, Output: admin@F5…
05/01/2017 19:47:18	279	sunil	Auto Implementation	Device: 41.101, Command: create ltm virtual vs_intra_443 destination…
05/01/2017 19:47:18	279	sunil	Auto Implementation	Device: 41.101, Command: create ltm pool pool_intra_443 load-balan…
05/01/2017 19:47:18	279	sunil	Auto Implementation	Device: 41.101, Command: create ltm profile http prof_http_intra_443…
05/01/2017 19:47:18	279	sunil	Auto Implementation	Device: 41.101, Command: create ltm monitor http mon_http_intra_4…
05/01/2017 19:47:18	279	sunil	Auto Implementation	Device: 41.101, Command: create cli transaction, Output: [batch mode
05/01/2017 19:47:12	279	sunil	Auto Implementation	Device: 41.101, Command: tmsh, Output: admin@F5v10_41(Active)(t…

The work order summary below the logs provides an overview of the workflow and time spent at each stage.



On successful completion of the work order, the ServiceNow change request **State** is updated to **Closed Complete**.

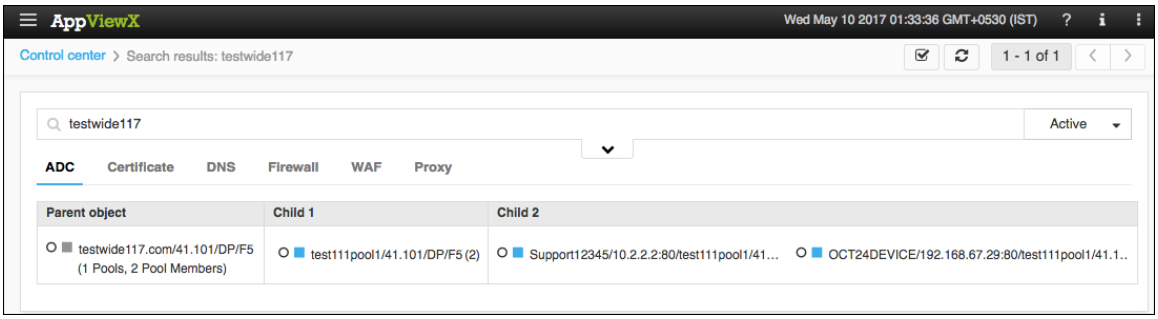


Roll Back

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Provisioning > Request**.
2. Locate the submitted request you want to review, then click the **Request ID number** to open the details page.
3. Click the **Work order** tab.
4. Select the check box beside the work order you want to roll back.
5. Click the  (**Rollback**) button in the Command bar to rollback all the configuration changes that were implemented.

Monitor and Manage

1. In the navigation menu on the left-hand side of the AppViewX screen, navigate to **Control center**.
2. In the **Search** field, enter the virtual server name to view a summary of the deployed application, the virtual server, and the associated pool and pool members.



3. Click the virtual server to open a topological view of the application that shows the virtual servers and their objects spread across different geographical locations and data centers.

   Note: This view contains action buttons that allow you to modify a few commonly tweaked load-balancing configurations, like the load balancing algorithm and the load distribution ratio.

4. Right-click any object in the topology to perform object-level basic operations on it, like disabling, backing up, restoring, and viewing configurations and logs.