



# **Zero Touch Provisioning (ZTP) of BIG-IP VE 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](http://www.centos.org)).

This product includes software developed by Red Hat, Inc. ([www.redhat.com](http://www.redhat.com)).

This product includes software developed by VMware, Inc. ([www.vmware.com](http://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](mailto:info@appviewx.com)

Web: [www.appviewx.com](http://www.appviewx.com)

**Document Information**

Software Version: 12.3.0

Document Version: 1.1

Last updated on: April 06, 2018

## Contents

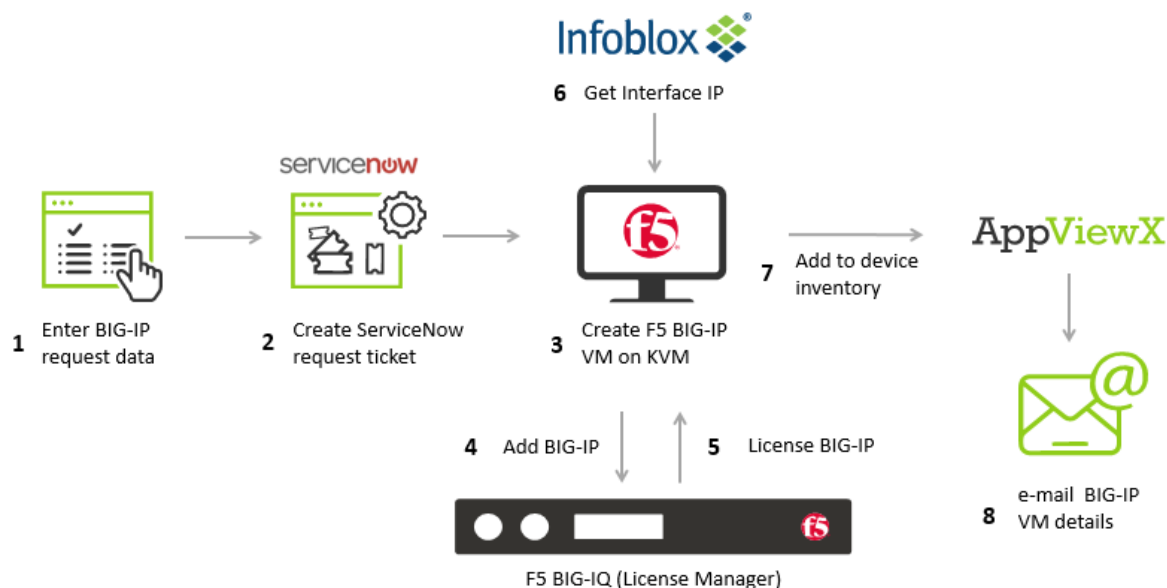
Description .....	1
Prerequisites .....	1
Compatible Software Versions .....	2
Limitations.....	2
Log In to AppViewX .....	2
Import Visual Workflows.....	3
Import Helper Scripts .....	3
Add a KVM Hypervisor.....	4
Add an ADC Device: BIG-IQ .....	5
Add a Server .....	7
Add an IPAM Device: Infoblox.....	8
SMTP Configuration.....	9
Register an ITSM Device: ServiceNow .....	10
Enable a Workflow .....	11
ZTP of BIG-IP VE Workflow .....	12
Work Order Flow .....	15
Rollback a workflow .....	17
WorkOrder flow .....	17
Request Inventory .....	18
Schedule a Workflow .....	19
View Scheduled Workflows .....	19
Add a Credential .....	20
Troubleshooting .....	20

## Description

The Zero Touch Provisioning (ZTP) of BIG-IP VE workflow is used to perform the following:

- Instantiate BIG-IP Virtual Edition (VE) on a KVM hypervisor.
- License using either a BIG-IQ or Bring Your Own License (BYOL) key.
- Integrate the workflow with an ITSM tool – ServiceNow for approvals and tracking.
- Do basic provisioning on the new BIG-IP and add it to the AppViewX inventory.
- Send email notifications regarding the implementation status and the new BIG-IP details.

The flow diagram shown below is designed to improve service efficiency and reduce manual effort.



## Prerequisites

To run the ZTP of BIG-IP VE workflow in your environment, ensure that the following prerequisites are met:

- Free AppViewX or AppViewX version 12.3.0 has been downloaded and installed.
- The following devices have been added to the AppViewX inventory:
  - KVM Hypervisor
  - BIG-IQ
  - DNS Name Server
  - NTP Server
  - SNMP Server
  - LDAP Server
  - Infoblox
- A storage pool (**/opt/vm/**) is available in KVM within which the guest VMs will be created.

- An image (.qcow2 format) of BIG-IP version 12.1 is available in the KVM home directory.
- KVM has at least 2 bridges to the external network. One will be used for device management and the other for the VLAN connection.
- The subnet of an additional interface is managed by the Infoblox IPAM.
- The management interface given to the VM has a proper DHCP in order to assign an IP address that will be used to access it.
- The following packages are available in KVM:
  - nmap
  - routes
  - brctl
  - virsh
- An ITSM device (ServiceNow) has been configured under the Change Management section of the AppViewX Settings module.
- If the user prefers not to use BIG-IQ, then they have their own registration key.
- The BIG-IQ has a registration key pool with free licenses activated in it.
- The time zone of the BIG-IQ and the new BIG-IP VE must be maintained. A device will be added whenever the time difference between the new VE and the BIG-IQ is more than 300 seconds.
- An SMTP server has been configured under System settings in order to receive email notifications. For more details on how to configure an SMTP server, refer to the [SMTP Configuration](#) section of this guide.

## Compatible Software Versions

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

- AppViewX – Free AppViewX and AVX 12.3.0
- ServiceNow – Geneva, Eureka, Jakarta, and Istanbul
- Infoblox – version 7.2.X
- F5 (both LTM and GTM) – version 10.x, 11.x, or 12.x

## Limitations

Not applicable

## Log In to AppViewX

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



`https://hostname:portnumber.`

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

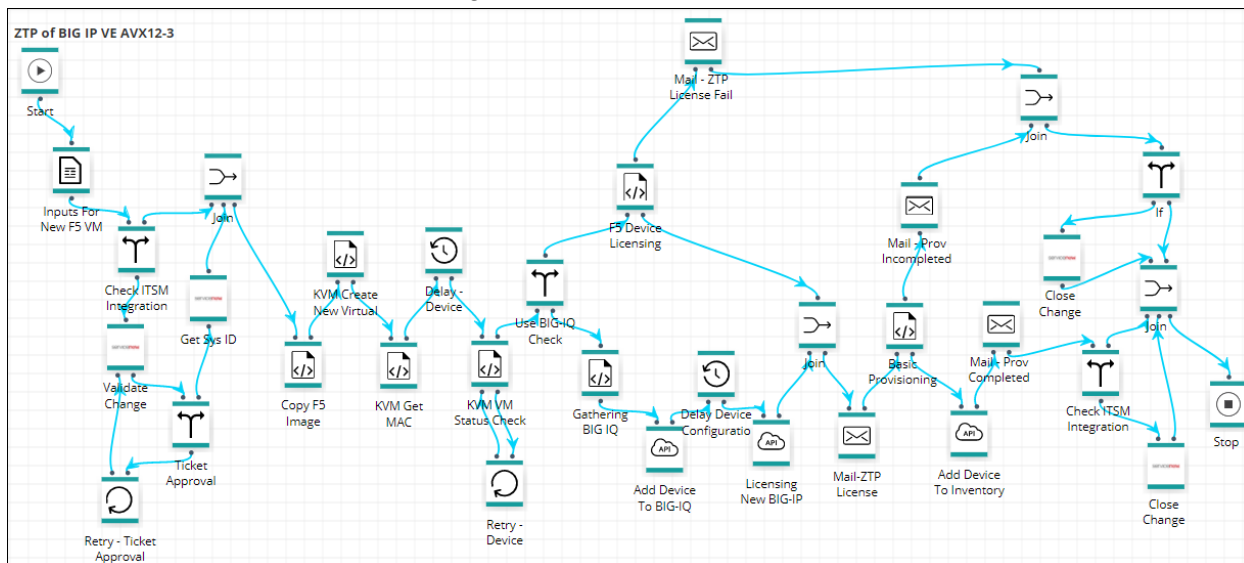
**Note:** It is recommended that you access AppViewX using Internet Explorer, Firefox, or Google Chrome.

## Import Visual Workflows

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




1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click the  (**Import**) button in the Command bar.
4. On the *Import* screen that opens, complete the following steps:
  - a. Click the **Browse** button.
  - b. Select the zip file containing one or more workflows, then click **Upload**.
  - c. In the table at the bottom of the Import page, select the check box beside the unzipped workflow file.
  - d. Click **Submit** to deploy the workflow into your AppViewX environment.

The ZTP of BIG-IP VE workflow diagram is shown below:



## Import Helper Scripts

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

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click on the  (**Helper script**) button in the Command bar.  
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.

- Click **Upload** to import the file and view its contents.

Status	Script name	Logs
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.

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

## Add a KVM Hypervisor

To a KVM hypervisor, complete the following steps:

- Click the (Menu) button on the left-hand side of the AppViewX screen
- Navigate to **Inventory > Device**.

The *Device* screen opens with **ADC** tab displayed by default.

- Click the **Others** tab.

**Note:** Devices (such as Windows and Linux machines) that are not supported by AppViewX are managed in the *Others* section.

- Click the (**Add**) button in the Command bar.

- On the *Add* screen that opens, enter a name for the device to help the users identify it.
- In the **IP address** field, enter the IP address of a device for which the connection must be established.

7. In the **Port** field, enter a port number through which you want to establish a network connection.
8. (Optional) In the **Model** field, enter a model name of the router. For KVM hypervisors, the model name should be KVM.
9. Enter a description of the device that makes it easy for users to tell what the device is for.
10. In the **Data center** field, enter the data center name in which the device resides.
11. 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. After you select a credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
12. Click **Save**. The new device is added to the AppViewX inventory and appears in the table on the *Others* tab.

Name	IP address	Access type	Model	Data center	Status
KVM	192.168.133.108	SSH:22	KVM	DC	Managed

The device will display one of the following statuses:

- **In Progress** – Device configuration fetch is in progress.
- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added 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 ADC Device: BIG-IQ

To add an ADC device, complete the following steps:

1. Click the (**Menu**) button on the left-hand side of the AppViewX screen
2. Navigate to **Inventory > Device**.
3. The *Device* screen opens with **ADC** tab displayed by default.
4. Click the (**Add**) button in the Command bar.

On the *Add* screen that opens, click to select **BIG-IQ** as the ADC vendor.



AppViewX Wed Oct 04 2017 12:40:02 GMT+0530 (IST)

Device :: ADC > Modify

**Device details** Device group

**Vendors**

BigIQ

**General information**

\* Device name Big-IQ-41.63 \* IP address 192.168.41.63

Data center DC Cert sync ☐ Managed ☐ Monitored ☒ Ignored

AppViewX group sync ☐

**Credentials**

\* Credential type Manual entry

\* User name admin \* Password .....

Save Cancel

5. In the **Device name** field, enter a name for the device to help users identify it.
6. In the **IP address** field, enter the IP address of a device for which the connection must be established.
7. (Optional) In the **Data center** field, enter the data center name in which the device resides.
8. 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. After you select a credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
9. Click **Save** and the **Device group** tab will be enabled.
10. From the list of group names, select the group to which you want to associate the device.
11. Click **Save**. The new BIG-IQ device is added to the AppViewX inventory and will be displayed in the collection grid under **ADC** tab.

AppViewX Wed Oct 04 2017 12:23:21 GMT+0530 (IST)

Device :: ADC

ADC Server DNS Firewall WAF Switch Router Proxy Others Cloud

Search...

Name	Sync group/cluster	IP address	Port	Vendor	Modules	Status	Data center
192.168.41.237		192.168.41.237	22	F5	LTM	Managed	DC
Big-IQ-41.63		192.168.41.63	22	BigIQ	LTM	Failed	DC
Device-asm-testing		192.168.133.141	22	F5	LTM,GTM	Unresolved	DataCenter

1 to 6 of 6



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.

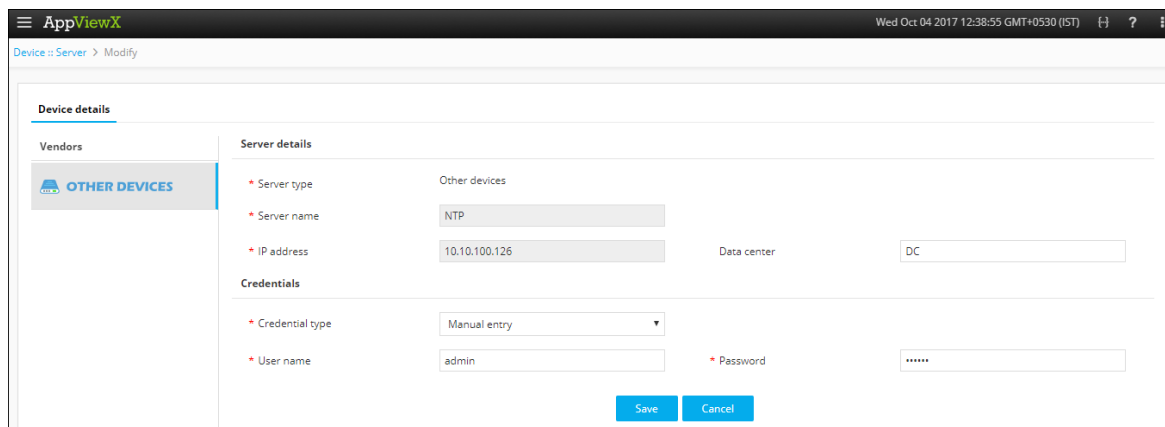
- **Failed** – Device configuration fetch failed, due to unsupported version.

## Add a Server

To add a server, complete the following steps:

1. Click the  (**Menu**) button on the left-hand side of the AppViewX screen
2. Navigate to **Inventory > Device**.  
The *Device* screen opens with **ADC** tab displayed by default.
3. Click the **Server** tab.
4. Click the  (**Add**) button in the Command bar.

On the *Add* screen that opens, click to select **Other Devices** and add the servers such as DNS Name Server, NTP Server, SNMP Server, and LDAP Server.



5. In the **Server name** field, enter a name for the server to help users identify it.
6. In the **IP address** field, enter the IP address for which the connection must be established.
7. (Optional) In the **Data center** field, enter the data center name in which the device resides.
8. 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. After you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
9. Click **Save**. The new server is added to the AppViewX inventory and appears on the *Server* tab.

Name	IP address	Data center	Vendor	Status	Credential type
Dummy	192.161.23.65	DC	Other Devices	Unresolved	Manual entry
KVM	192.168.133.108	DC	Other Devices	Managed	Manual entry
NTP	10.10.100.126	DC	Other Devices	Unresolved	Manual entry

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

To add an IPAM device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Inventory > Device**.  
The *Device* screen opens with **ADC** tab displayed by default.
3. Click the **DNS** tab.
4. Click the (**Add**) button in the Command bar.

On the *Add* screen that opens, click to select **Infoblox** as the DNS vendor.

**Device details**

**Vendors**

- Infoblox

**General information**

\* Grid master: test

\* FQDN/IP address: 192.168.40.229

Data center:

**Credentials**

\* Credential type: Manual entry

\* User name: admin

\* Password:

**Secondary device information**

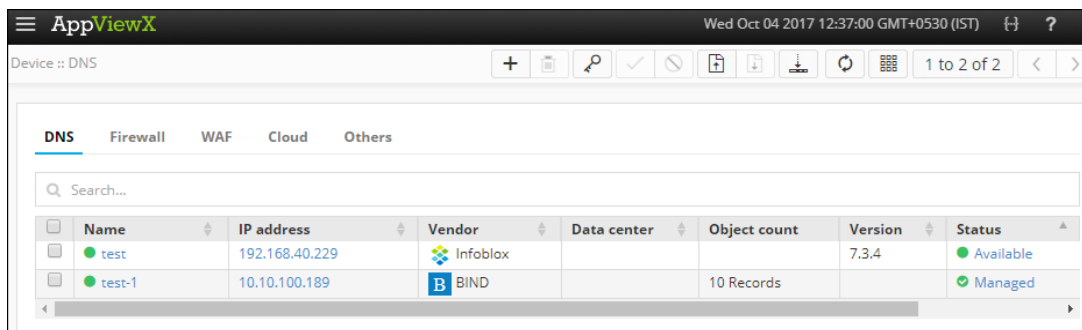
Grid master candidate: ☐

Save Cancel

5. In the **Grid master** field, enter a name for the primary device to help users identify it.
6. In the **FQDN/IP address** field, enter the IP address of the primary device for which the connection must be established.

7. (Optional) In the **Data center** field, enter the data center name in which the device will reside.
8. 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 primary 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. After you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
9. Click **Grid master candidate** checkbox if you want to add a secondary device.
10. At a minimum, fill in all fields that contain a red asterisk beside their names.
11. Click **Add** to add the secondary device to the table at the bottom of the screen.
 

**Note:** You can add more than one secondary device. The **Update** and **Delete** buttons are enabled only when you try to modify existing secondary devices.
12. Click **Save**. The new device is added to the AppViewX inventory and appears on the **DNS** tab.



The screenshot shows the AppViewX web interface. At the top, there's a header with the AppViewX logo and a timestamp 'Wed Oct 04 2017 12:37:00 GMT+0530 (IST)'. Below the header, there's a navigation bar with tabs: DNS, Firewall, WAF, Cloud, and Others. The 'DNS' tab is selected. Below the navigation bar, there's a search bar labeled 'Search...'. Below the search bar, there's a table with the following columns: Name, IP address, Vendor, Data center, Object count, Version, and Status. The table contains two rows: one for 'test' with IP 192.168.40.229, Vendor Infoblox, and Status Available; and one for 'test-1' with IP 10.10.100.189, Vendor BIND, Object count 10 Records, and Status Managed.

Name	IP address	Vendor	Data center	Object count	Version	Status
test	192.168.40.229	Infoblox			7.3.4	Available
test-1	10.10.100.189	BIND		10 Records		Managed


The device will display one of the following statuses:

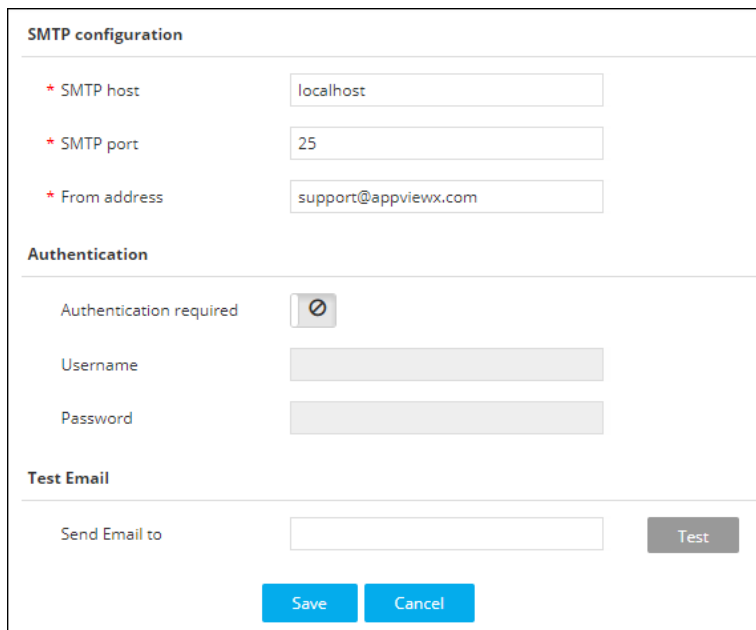
- **In Progress** – Device configuration fetch is in progress.
- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device, due to invalid login credentials.
- **Failed** – Device configuration fetch failed, due to unsupported version.

## SMTP Configuration

The System tab within the Settings module is where you configure the Simple Mail Transfer Protocol (SMTP) server details for sending an email notification.

To configure an SMTP server, complete the following steps:


1. Click the  (**Menu**) button.
2. Navigate to **Settings > General > SMTP**.



The image shows a web form titled "SMTP configuration". It is divided into three sections: "SMTP configuration", "Authentication", and "Test Email".

- SMTP configuration:** Contains three input fields with red asterisks indicating they are required:
  - SMTP host:** A text input field containing "localhost".
  - SMTP port:** A text input field containing "25".
  - From address:** A text input field containing "support@appviewx.com".
- Authentication:** Contains:
  - Authentication required:** A toggle switch currently in the "off" position, labeled "Disabled".
  - Username:** A text input field.
  - Password:** A text input field.
- Test Email:** Contains:
  - Send Email to:** A text input field.
  - Test:** A grey button.

At the bottom of the form are two blue buttons: "Save" and "Cancel".

3. In the **SMTP host** field, enter the host address of the SMTP server.
4. In the **SMTP port** field, enter the port number for the SMTP server.
5. In the **From address** field, enter the email address from which the notification must be sent.
6. If an SMTP server requires authentication to connect, click the  (**Disabled**) button to enable it.
7. If you enabled authentication in Step 6, enter the user name and the associated password that is used for authentication on the SMTP server.
8. In the **Send Email to** field, enter an email address to whom you want to send a notification.
9. Click the **Test** button. If the configuration is successful, a test email will be sent to the address (you provided in step 8) verifying the status of configuration.
10. Click **Save** to save the changes you have made to the system settings.

## 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.

Settings :: Change Management > Vendor configuration

**Authentication**

SSH

Certificate

Provisioning

**Change Management**

ADC

Backup & Restore

Log forwarding

License

System

AppViewX

**Information**

Name: Change

URL: https://ven01189.service-now.com

Description: [Empty field]

Upload image: [Image upload button]

Username: admin

Password: [Password field]

**General settings**

Active Provisioning Instance: ☒

Device / CI validation: ☐

Timezone: GMT

Implementation mode: Stop

Enable polling: ☐

Polling interval (mins): 5

Approve mode: Stop

**Log / Configuration settings**

Select configuration type: Pre validation, Post validation

Consolidated logs: ☒

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.

serviceNOW Service Automation

Welcome: System Administrator

Logout

Search

Load Balancer - 112.40

Update Delete

Name: SFO\_F5\_ADC\_R23

Company: [Empty field]

Asset tag: [Empty field]

Serial number: [Empty field]

Manufacturer: [Empty field]

Model ID: [Empty field]

Asset: [Empty field]

Assigned to: [Empty field]

IP Address: 192.168.40.153

Host name: [Empty field]

Configuration

Load Balancers

LB Hardware

LB Applications

MID Server

Downloads

System Definition

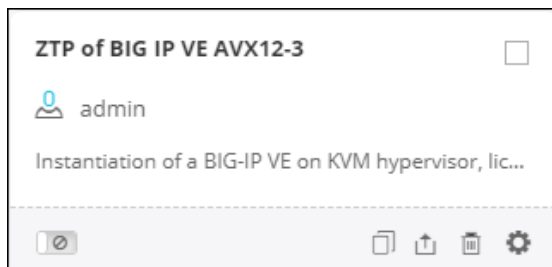
Upload File

## Enable a Workflow

To enable the ZTP of BIG-IP VE workflow, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow > Studio**.  
The *Workflow* screen opens.
3. Click the (**Select**) button on the ZTP of BIG-IP VE workflow to enable. If the workflow is already selected, a (**Deselect**) button appears.
4. Click the (**Enable**) button in the Command bar.


**Note:** You can also enable the ZTP of BIG-IP VE workflow from the Card view by clicking the (**Disable**) button.



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

## ZTP of BIG-IP VE Workflow

To submit the ZTP of BIG-IP VE 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 Play button on the ASM Policy Migration workflow to execute.



The *Form Builder* screen opens with the **Request View** tab displayed by default.

Request :: Inventory > ZTP of BIG-IP VE AVX12-3 :: FormBuilder

Request View

Workorder View

▶

⚙️

Inputs for New F5 VM

\* Select Host Machine

Select

⌵

ⓘ

\* VM Name

?

\* Use BIG-IP Flavours?

☒ Yes ☐ No

\* BIG-IP Flavour

Small - 1SLOT (2vCPUs / 4096M-RAM / 20G...

⌵

?

Get Management Interface

\* Management Interface

Select

⌵

?

Get Additional Interface

\* Additional Interface

Select

⌵

?

\* Use BIG-IQ for Licensing?

☒ No ☐ Yes


?

\* Base Registration Key

?

\* First Name




\* Last Name

4. In the **Select Host Machine** field, click the  (**Retrieve field values**) button to fetch the list of host machines. Select the host machine for which you want to create a guest Virtual Machine (VM).
5. In the **VM Name** field, enter a name for the F5 VM to help the users identify it.
6. In the **Use BIG-IP Flavors** field, select how you want to configure the guest VM:
  - a. Select **Yes** to use the BIG-IP Flavor configurations that are provided by F5.
  - b. Select **No** to manually enter the CPU Cores and RAM size of the guest VM.
7. Click the **Get Management Interface** button to retrieve the list of interfaces available in the host machine.
8. From the **Management Interface** dropdown list, select the interface you want to use for configuration and management operations.
9. Click the **Get Additional Interface** button to retrieve the list of interface available in the host machine.

This will display all the interfaces except the ones that are used for management operations.




10. From the **Additional Interface** dropdown list, select the interface you want to use for external network handling (VLAN configuration).

**Note:** We are adding only one additional interface to this workflow.


11. If you do not want to use a BIG-IQ device for licensing, select **No** and do the following:
  - a. In the **Base Registration Key** field, enter the registration license key you received from F5 in order to communicate with the device.
  - b. Enter the details (such as first and last name, job title, company name, address, phone number, email address, host name, password, and time zone) in order to get a license from F5.
12. If you want to use a BIG-IQ device for licensing, select **Yes** and do the following:
  - a. In the **Select BIG-IQ Device** field, click the  (**Retrieve field values**) button to fetch the list of BIG-IQ devices. Select the BIG-IQ device you want to use for licensing.
  - b. In the **BIG-IQ Device Pool** field, click the  (**Retrieve field values**) button to fetch the list of pools available in the BIG-IQ device. Select the pool you want to use from the BIG-IQ Device.
  - c. In the **Registration Key Pool** field, click the  (**Retrieve field values**) button to fetch the list of registration key pools available in the BIG-IQ device. Select the license key pool from the dropdown list.
  - d. Enter the details (such as host name, admin password, and time zone) in order to get the license from BIG-IQ.
13. From the **Provisioning Modules** dropdown list, select the modules you want to provision.

**Note:** This option appears only when you manually enter the configuration details of the guest VM.



14. In the Infoblox device field, click the  (**Retrieve field values**) button to fetch the list of Infoblox devices present in the AppViewX inventor. Select the device you want to integrate with the workflow from the dropdown list. This allows users to reserve a free IP address from the available address pools, which you can use later to tag with the VLAN.
15. In the **Vlan name** field, enter a name for the VLAN connection to help users identify it.
16. In the **NTP Server** field, click the  (**Retrieve field values**) button to fetch the list of NTP servers present in the AppViewX inventory. Select the NTP server you want to use for time synchronization.
17. In the **DNS Name Server** field, click the  (**Retrieve field values**) button to fetch the list of DNS name servers present in the AppViewX inventory. Select the DNS server you want to use for DNS resolution.
18. Depending on whether or not you want to configure an **SNMP server** for the guest VM, click the **Yes** or **No** radio button. To configure an SNMP server, do the following:
  - a. Click the **Get SNMP Servers** button to retrieve the list of SNMP servers from the AppViewX inventory. Select the host you want to use for network management from the **SNMP Host** dropdown list.
  - b. Enter the **Community**, **Trap name**, and **port** details of the selected SNMP server in the respective fields.
19. Depending on whether or not you want to configure an **LDAP server** for the guest VM, click the **Yes** or **No** radio button. To configure an LDAP server, do the following:
  - a. Click the **Get LDAP Servers** button to retrieve the list of LDAP servers from the AppViewX inventory. Select the server you want to use for authentication from the **LDAP Server** dropdown list.
  - b. Enter the **Port**, **Domain**, and **password** of the selected LDAP server in the respective fields.
20. In the **Device Name for AVX Inventory** field, enter a name for the device. The device name should be same as how it is mentioned in the AppViewX inventory.

21. Depending on whether or not you want to integrate **ServiceNow** (SNOW), select the **Yes** or **No** radio button. To integrate ServiceNow, you must enter the following details:

- a. Click the  (**Calendar**) button to select the start and end dates and times for the service window. The configuration changes will be implemented during this timeframe.
22. Click the **Create ServiceNow Ticket** button to retrieve the ticket number. A new request ID automatically appears in the **Ticket Number** field.
23. From the **Business Unit** dropdown list, select the business unit from where you want the workflow to be triggered.
24. In the **Mail ID** field, enter an email address of the recipient to whom you want to send the status of the workflow.
25. Click **Submit**.

To view the request details refer to the Request Inventory section of this guide.

## Work Order Flow

Following are the workorder tasks of ZTP of BIG-IP VE workflow.

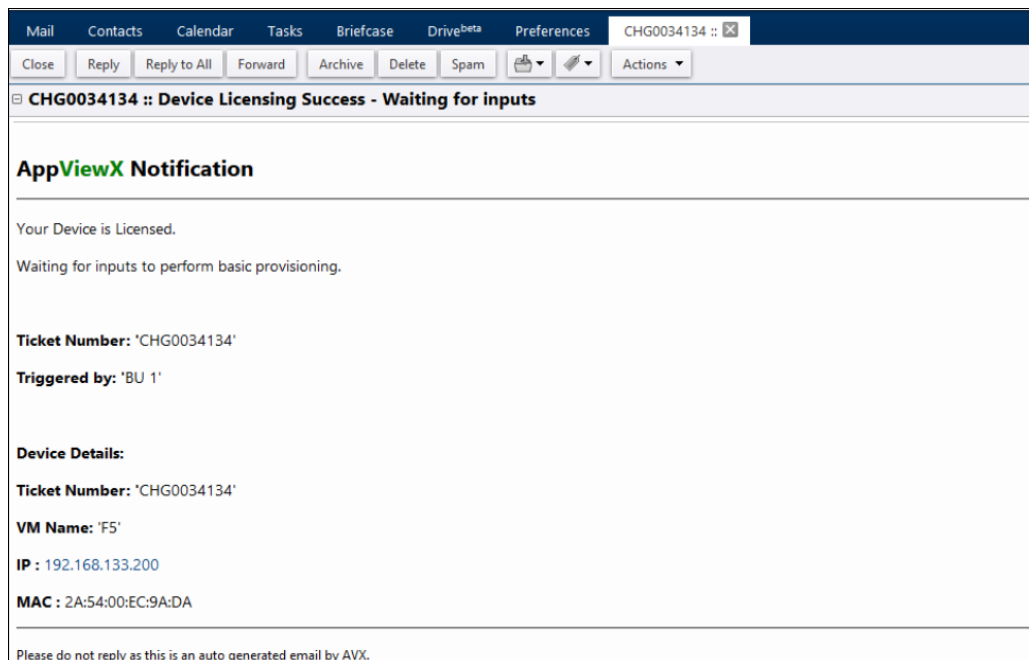
**Note:** You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.

1. **Copy F5 Image** — An image (**qcow2** format) is copied from the KVM home directory to the storage pool **/opt/vm**
2. **KVM Create New Virtual Machine** — A new VM is created based on the input provided in the form builder.
3. **KVM Get MAC Information of the VM** — The MAC information of the guest VM is provided when the commands are run on the host.
4. **Delay Device Configuration** — A one-minute delay is added to give time for the VM configuration. It is also based on the speed of the KVM. If the KVM is already loaded, the delay time will vary.
5. **KVM VM Status Check** — The status check ensures that the device is up and running. The IP address of the guest VM is obtained.
6. **Gathering BIG-IQ Information** — The BIG-IQ device information is gathered to license the VM.
7. **Add Device to BIG-IQ** — A device is added to BIG-IQ based on the inputs provided in the form builder.
8. **F5 Device Licensing**

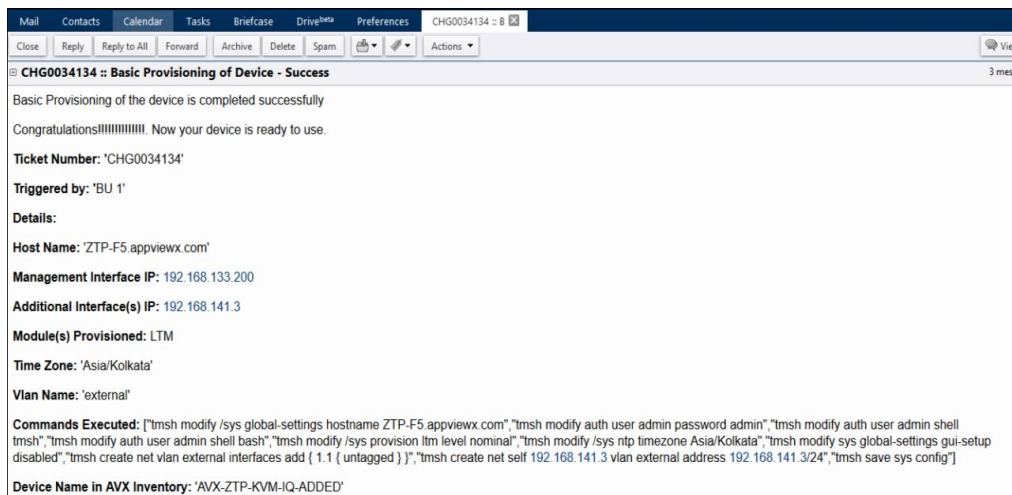
If the user selected BYOL, the license key will communicate to the device to get the dossier key. This dossier key is then sent to *activate.f5.com*, which returns the license. The license is then pushed to the device and activated.

If the user selected BIG-IQ, a free license is obtained from the license key pool. The new BIG-IP VE is added to the BIG-IQ device as a managed entity and the license from the selected key pool is provided to the device.

9. **Mail-ZTP License Success** — An email notification on the status of the BIG-IP VE licensing is sent to the users.





10. **Basic Provisioning** — The BIG-IP VE is provisioned for external network handling based on the details provided in the form builder.
11. **Add Device to Inventory** — The BIG-IP VE device is added to the AppViewX ADC device inventory.
12. **Mail - Prov Completed** — An email notification on the status and details of the BIG-IP VE provisioning is sent to the users.



## Rollback a workflow

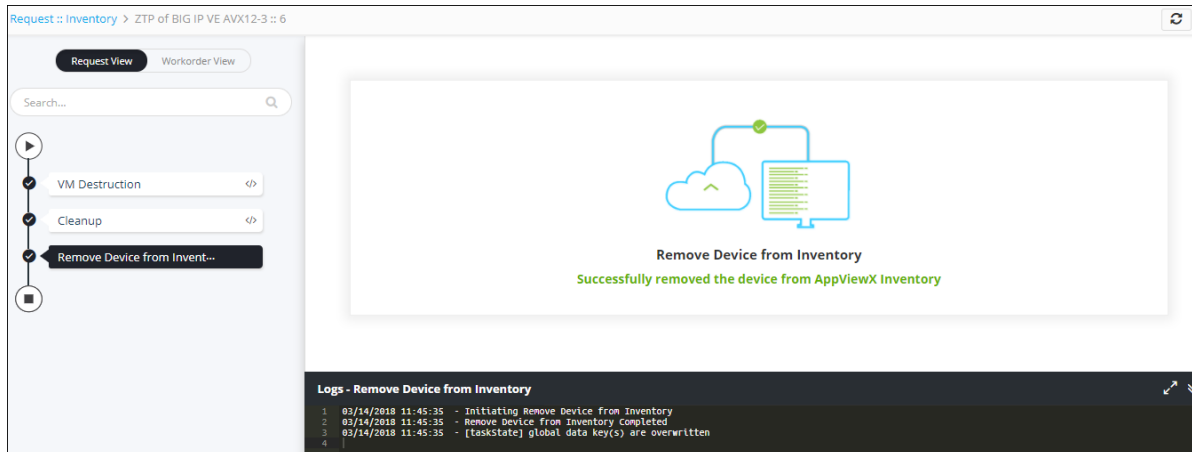
A rollback action can be performed only on the completed workflows. To trigger a rollback action, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Workflow > Request**.  
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 created for ZTP of BIG-IP VE workflow using the **Search** field and/or click the  (**Filter**) button.
4. Right-click the request and select **Rollback**.
5. On the Confirmation screen that appears, click **Yes**.
6. Select the **Request** or **Workorder** radio button based on how you want to set the rollback type.
7. Click **Rollback** to trigger the action.

## WorkOrder flow

The following are the workorder tasks of ZTP of BIG-IP VE workflow, when you perform a rollback action:

**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. **VM Destruction** — The BIG-IP VM in the KVM hypervisor is destroyed.
2. **Cleanup** — The IP address reserved in the Infoblox device is released. If the license was allocated from the BIG-IQ license pool, it revokes the license and adds it back to the BIG-IQ license pool.
3. **Remove Device from Inventory** — The BIG-IP device is removed from the AppViewX device inventory.


## 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.

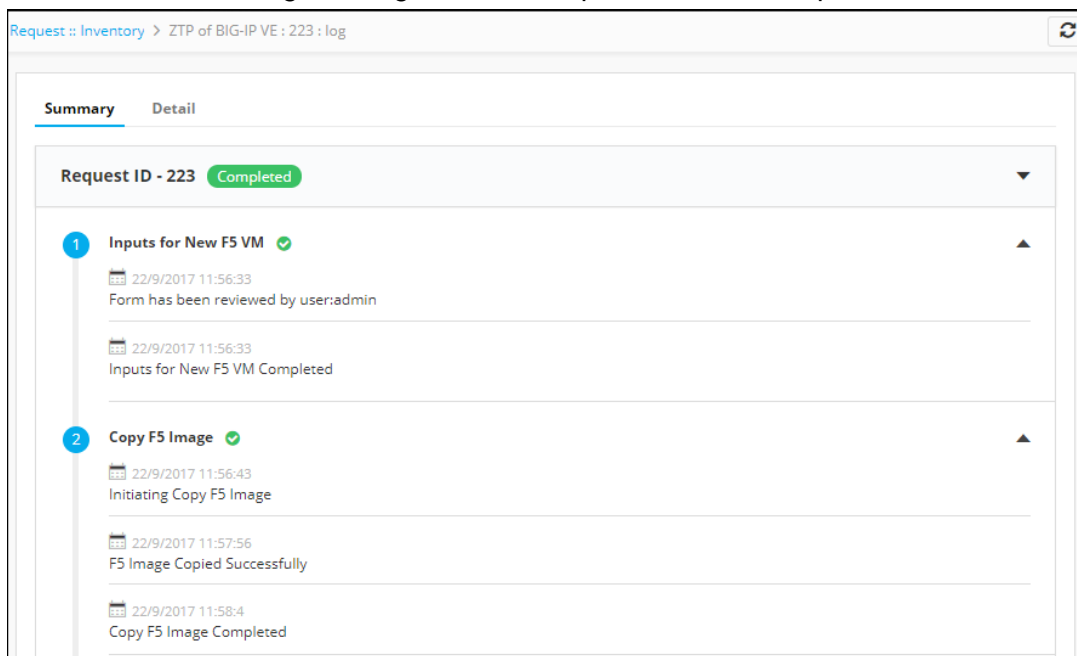
AppViewX							
Request Inventory							
My catalog Request Inventory Scheduled workflows							
Search...							
Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log	
229	Modify Virtual Server	admin	26/09/2017 03:00 PM	26/09/2017 03:00 PM	In Progress	<a href="#">View</a>	
228	ASM Policy Creation	admin	26/09/2017 03:00 PM	26/09/2017 03:00 PM	In Progress	<a href="#">View</a>	
227	ASM Policy Creation	admin	26/09/2017 02:58 PM	26/09/2017 02:58 PM	In Progress	<a href="#">View</a>	
226	ASM Policy Creation	admin	26/09/2017 02:53 PM	26/09/2017 02:53 PM	In Progress	<a href="#">View</a>	
225	ASM Policy Creation	admin	26/09/2017 02:47 PM	26/09/2017 02:47 PM	In Progress	<a href="#">View</a>	
224	ASM Policy Creation	admin	26/09/2017 02:41 PM	26/09/2017 02:41 PM	In Progress	<a href="#">View</a>	
223	ZTP of BIG-IP VE	admin	22/09/2017 11:56 AM	22/09/2017 11:56 AM	Completed	<a href="#">View</a>	
222	ASM Policy Migration	admin	22/09/2017 11:26 AM	22/09/2017 11:26 AM	Completed	<a href="#">View</a>	

4. Click the **Request ID** created for ZTP of BIG-IP VE to view its details.

The screen opens with the **Request View** tab selected by default.



- a. After the workflow execution is complete, the **Request View** tab displays the tasks or phases of a request in a tree view. For more details, refer to the [Work Order Flow](#) section of this guide.

- b. Click the **Workorder View** tab to view the work order details such as work order ID, date and time when the work order was created and updated, status, RFC ID, and RFC status.
5. In the *Request Inventory* screen, you can also view the following details of the request: request creator, request time, last updated time, status, and activity log.
6. Click the **View** link in the **Activity log** column to display the request in a stage view. In the **Summary** tab, click the  (**Expand**) icon to view the details of each task. Click the **Details** tab to view log messages and other particulars of a request.



## Schedule a 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 ZTP of BIG-IP VE workflow.
4. On the ZTP of BIG-IP VE window that opens, select the frequency of the policy migration process: once, hourly, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on what you select.
5. Click **Save**.

## View Scheduled Workflows


To go to the scheduled workflow screen, complete the following steps:


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

3. The *Request* screen opens with **My catalog** tab displayed by default.
4. Click the **Scheduled workflows** tab.
5. On the Scheduled workflow screen that appears, you can perform the following tasks:
  - In the **View log** column, click **View** to display the details of a scheduled workflow.
  - Click the  (Pause) or  (Resume) button to temporarily stop or continue the execution of a workflow.

## Add a Credential

To add a credential to a device, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Inventory > Device**.

The *Device* screen opens with the **ADC** tab selected by default.
3. Click the 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.

## Troubleshooting

### I cannot find the ZTP of BIG-IP VE 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.

### Why does BIG-IP VE licensing fail?

BIG-IP licensing fails in the following scenarios:

- When the license key is misspelled.
- When an incorrect license key pool is selected in Big-IQ.

When there is no Internet connection to connect to AppViewX, activate BYOL keys, and create a ServiceNow ticket.