AppViewX

Zero Touch Provisioning (ZTP) of BIG-IP VE

October 2017

Trademarks

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: 1.0

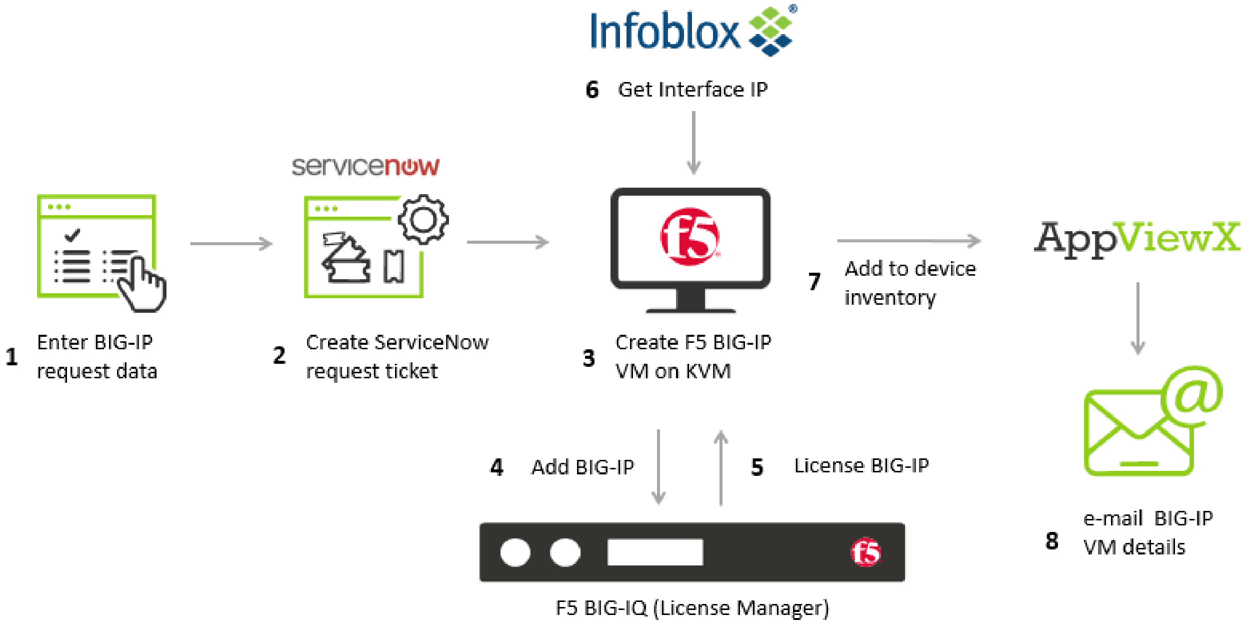
Contents

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.
- Use either a BIG-IQ or Bring Your Own License (BYOL) key for licensing.
- 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.

It will improve the service efficiency and reduce the manual effort. The ZTP of BIG-IP VE workflow is shown in the image below:


Infoblox
6 Get Interface IP
servicenow
AppViewX
1 Enter BIG-IP request data
2 Create ServiceNow request ticket
3 Create F5 BIG-IP VM on KVM
7 Add to device inventory
4 Add BIG-IP
5 License BIG-IP
8 e-mail BIG-IP VM details
F5 BIG-IQ (License Manager)

Prerequisites

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

- Free AppViewX or AppViewX version 12.1.0 and 12.2.0 is downloaded and installed.
- Following devices must have been added into the AppViewX inventory:
  - KVM Hypervisor
  - BIG-IQ
  - DNS Name Server
  - NTP Server
  - SNMP Server
  - LDAP Server
  - Infoblox
- Standard KVM conventions must be followed while you create a Virtual Machine (VM).

  Note: No special characters except hyphen (-) are accepted.

- A storage pool (**/opt/vm/**) must be available in KVM within which the guest VM(s) will be created.
- An image (**.qcow2** format) of BIG-IP version 12.1 must be available in the KVM home directory.
- KVM should have at least 2 bridges to the external network, out of which one will be used for device management and the other one for VLAN connection.
- The subnet of an additional interface should be managed by the Infoblox IPAM.
- The management Interface given to the VM must have a proper DHCP in order to assign an IP address for accessing it.
- Following packages must be available in KVM:
    - `nmap`
    - `routes`
    - `brctl`
    - `virsh`
- An ITSM device (ServiceNow), must have been configured under Change Management of AppViewX Settings.
- If the user prefer not to use BIG-IQ then he/she must have their Own Registration key.
- A BIG-IQ should have 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 when the time difference between the new VE and the BIG-IQ is more than 300 seconds.
- An SMTP server must have 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 section of this guide.

Compatible Software Versions

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

- AppViewX – Free AppViewX version and version12.1.0 and version12.2.0
- ServiceNow – Geneva version and Eureka version
- Infoblox – version7.2.X
- F5 (both LTM and GTM) – version10.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.

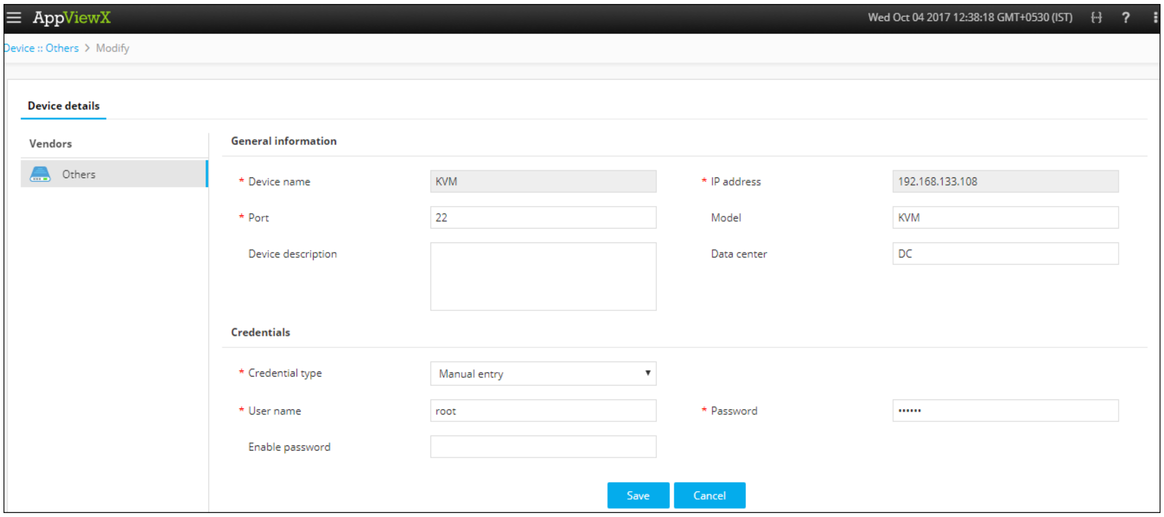
Add a KVM Hypervisor

To a KVM hypervisor, 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 **Others** tab.

   Note: Devices (such as Windows and Linux machines) that are not supported by AppViewX are managed in the *Others* section.
4. Click the + (**Add**) button in the Command bar.


AppViewX
Wed Oct 04 2017 12:38:18 GMT+0530 (IST)
Device :: Others > Modify
Device details
Vendors
Others
Save
Cancel

General information

* Device name: KVM

* IP address: 192.168.133.108

* Port: 22

Model: KVM

Device description:

Data center: DC

Credentials

* Credential type: Manual entry ▾

* User name: root

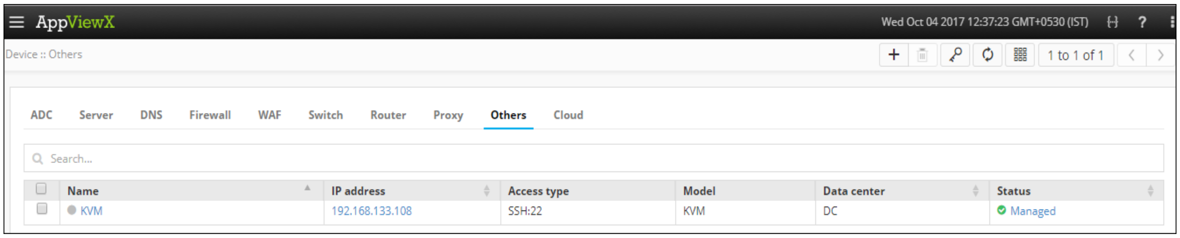
* Password: ••••••

Enable password:

5. On the *Add* screen that opens, enter a name for the device to help the users identify it.
6. 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 when 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.

You must select the credential name from the dropdown list and the **user name** and **password** fields will be auto-filled with the values provided while creating a Credential template.

12. Click **Save**. The new device is added to the AppViewX inventory and will be displayed in the collection grid under *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:

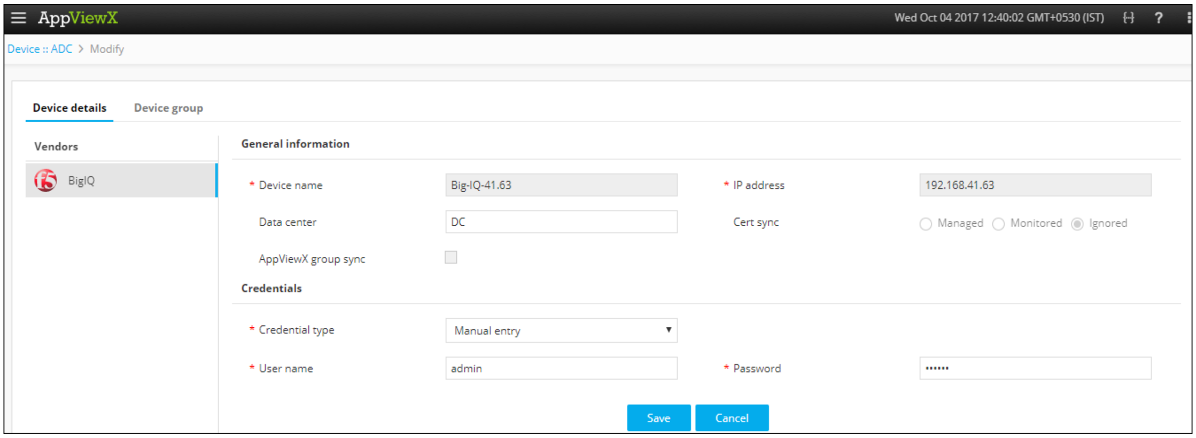
- **In Progress** – Device configuration fetch is in progress.
- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added device should have.
- **Unresolved** – Unable to communicate with device, due to invalid login credentials.
- **Failed** –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

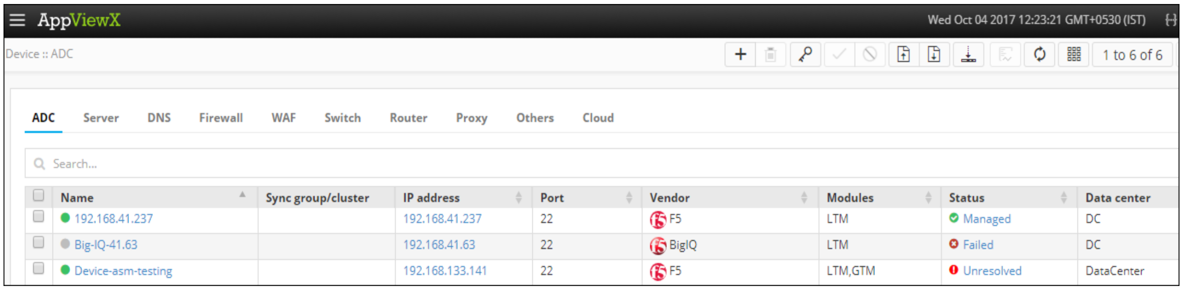


* Device name: Big-IQ-41.63
* IP address: 192.168.41.63
Data center: DC
Cert sync: ○ Managed ○ Monitored ● Ignored
AppViewX group sync: □
* Credential type: Manual entry
* User name: admin
* Password: ••••••

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 when 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.

      You must select the credential name from the dropdown list and the **user name** and **password** fields will be auto-filled with the values provided while creating a 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.



□	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

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.

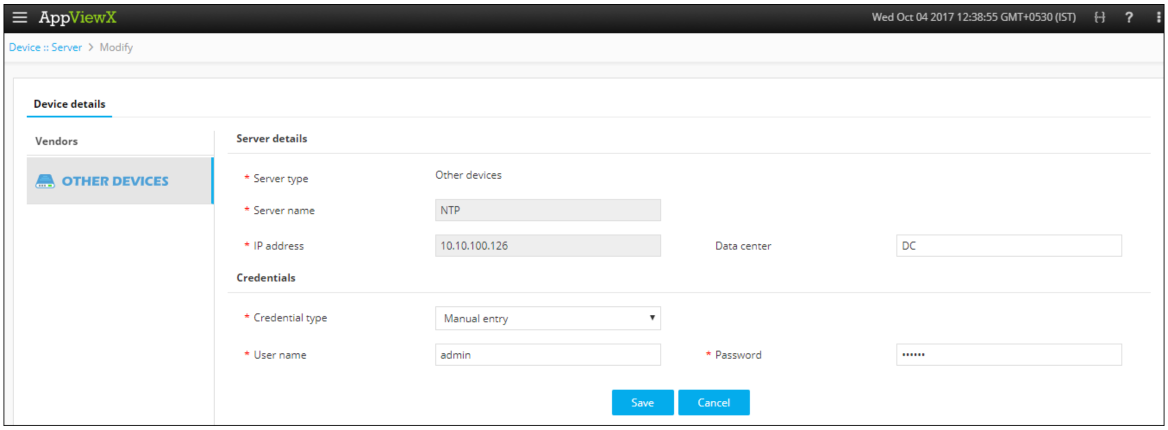
ADD a Server:

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.


AppViewX
Wed Oct 04 2017 12:38:55 GMT+0530 (IST)
Device :: Server > Modify
Device details
Vendors
OTHER DEVICES
Save
Cancel

Server details

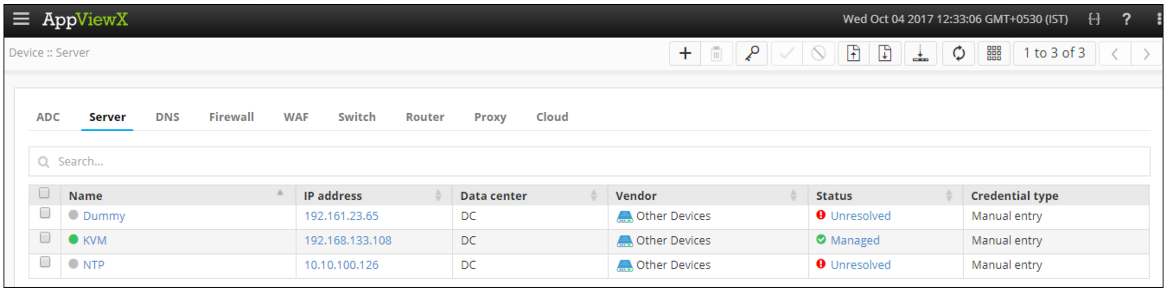
* Server type	Other devices		
* Server name	NTP		
* IP address	10.10.100.126	Data center	DC

Credentials

* Credential type	Manual entry		
* User name	admin	* Password	••••••

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 when 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.

      You must select the credential name from the dropdown list and the **user name** and **password** fields will be auto-filled with the values provided while creating a Credential template.
9. Click **Save**. The new server is added to the AppViewX inventory and will be displayed in the collection grid under *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.

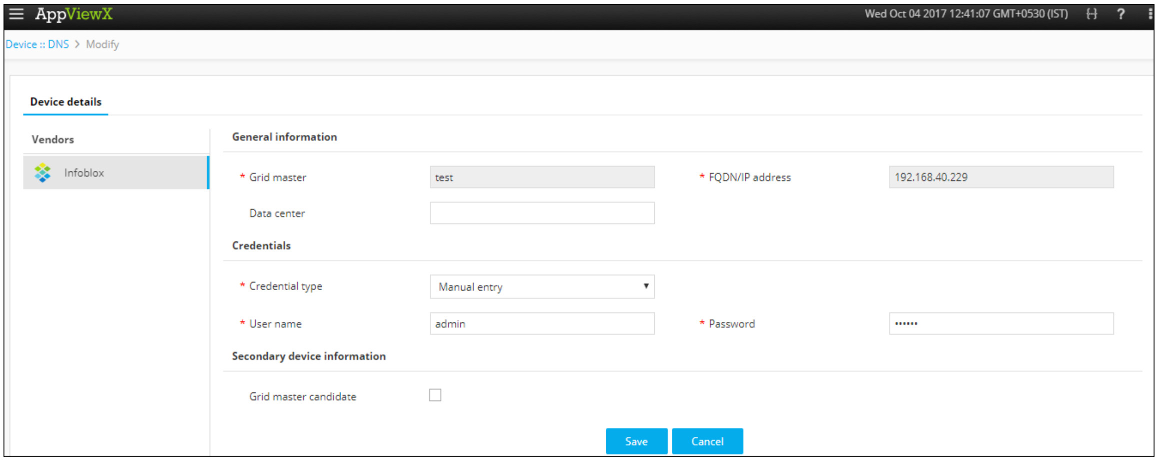
Add an IPAM Device: Infoblox

To add an IPAM device, complete the following steps:

1. Click the ☰ (**Menu**) button 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 **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.



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

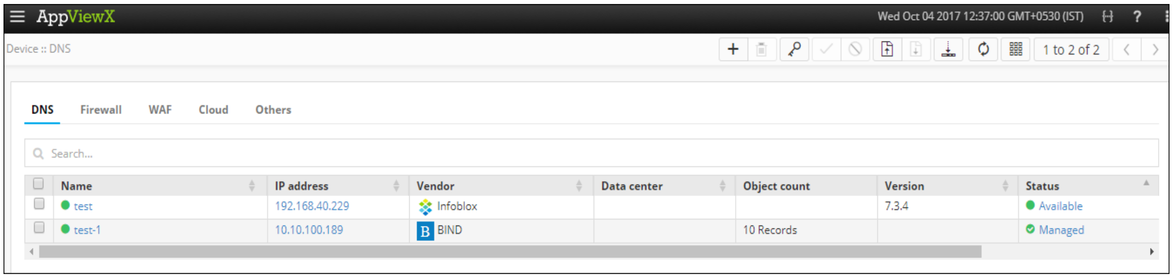
Grid master candidate □

5. In the **Grid master** field, enter a name for the primary device to help the 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 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 when 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.

     You must select the credential name from the dropdown list and the **user name** and **password** fields will be auto-filled with the values provided while creating a 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**. The secondary device will be displayed in the collection grid.

    Note: You can add more than one secondary devices. **Update/Delete** buttons will be enabled only when you try to modify the secondary device that are added.

12. Click **Save**. The new device is added to the AppViewX inventory and will be displayed in the collection grid under *DNS* tab.



□	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	B 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.

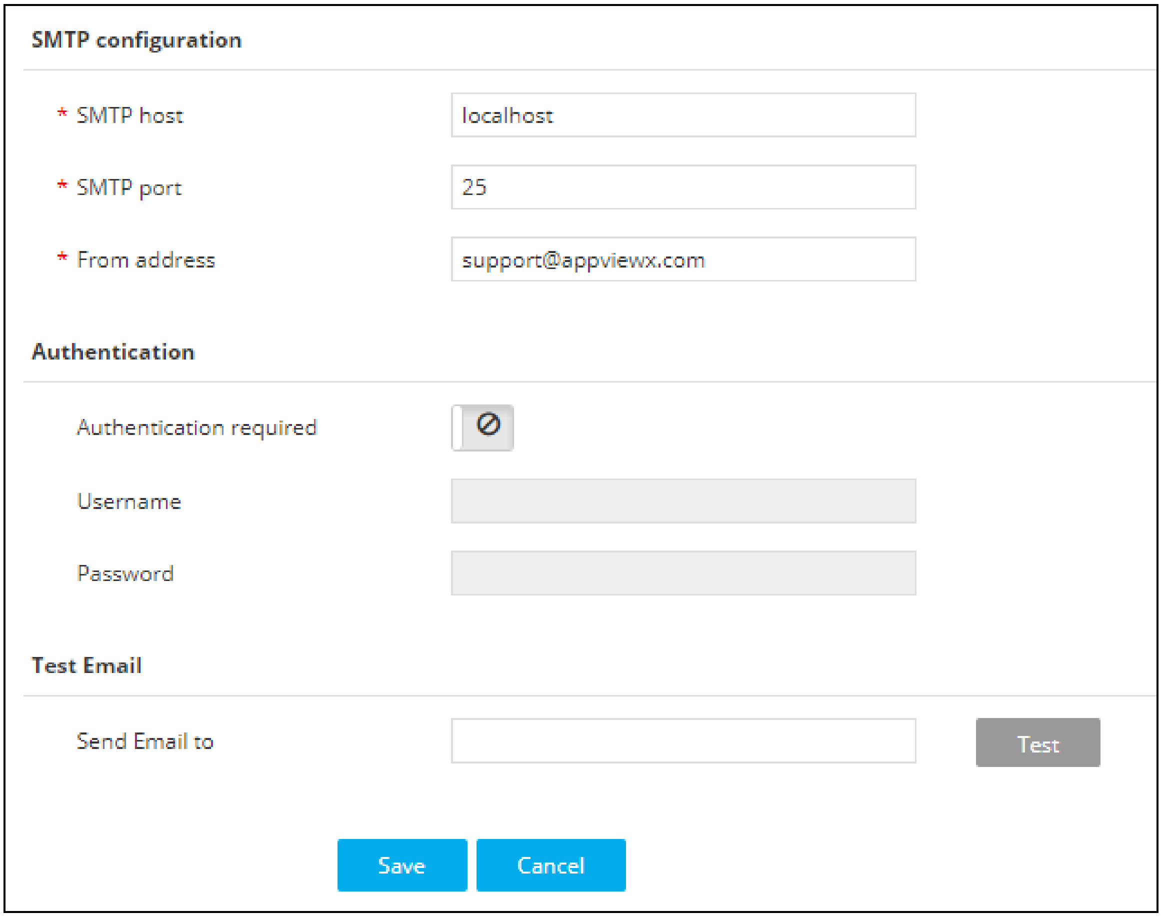
SMTP Configuration

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. Click the **Settings** option.

   On the *Settings* screen, click the **System** tab.



SMTP configuration

* SMTP host	localhost
* SMTP port	25
* From address	support@appviewx.com

Authentication

Authentication required	⊘
Username	
Password	

Test Email

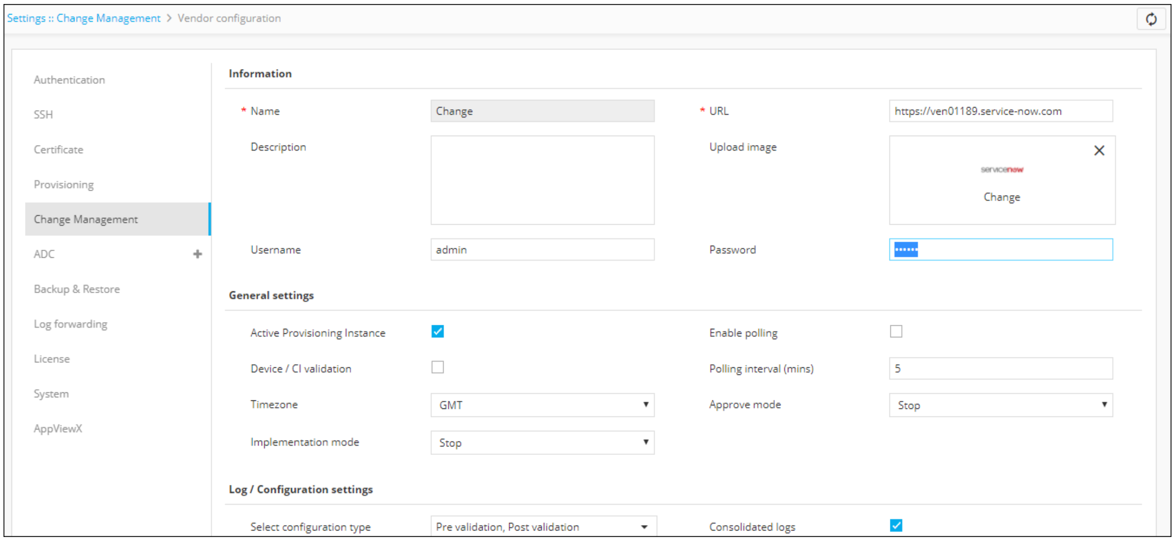
Send Email to	

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 authentication is required to connect to the SMTP server, click the ⊘ (**Disabled**) button to enable it.
7. If you enabled authentication in Step 6, enter the user name and the associated password used for authenticating 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. A test email verifying the status of configuration will be sent to the email address you provided on Step 8.
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.



Information

* Name	Change	* URL	https://ven01189.service-now.com
Description		Upload image	servicenow Change
Username	admin	Password	••••••

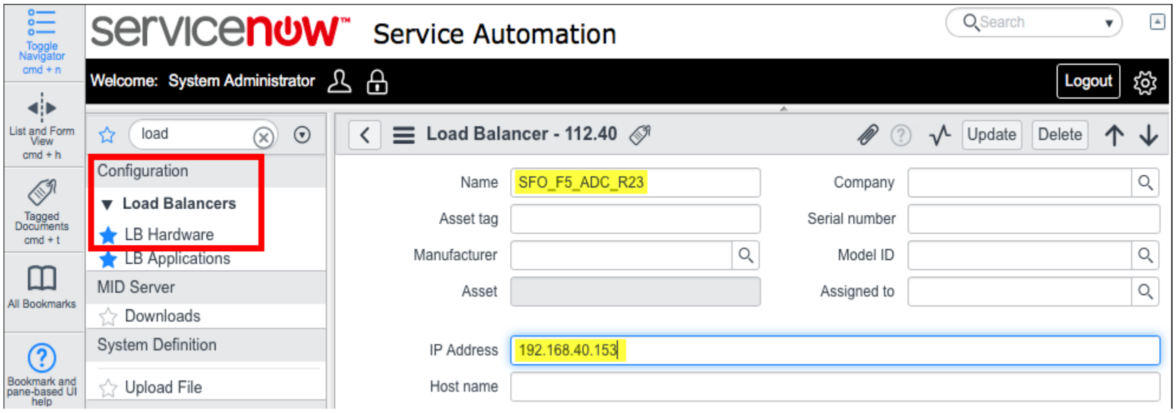
General settings

Active Provisioning Instance	☑	Enable polling	☐
Device / CI validation	☐	Polling interval (mins)	5
Timezone	GMT	Approve mode	Stop
Implementation 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 is shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.

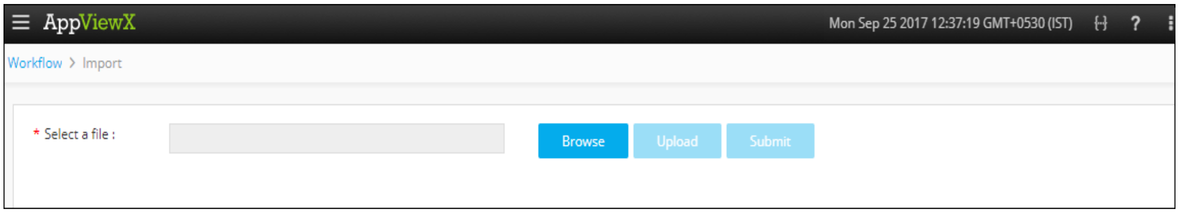


Name	SFO_F5_ADC_R23	Company	
Asset tag		Serial number	
Manufacturer		Model ID	
Asset		Assigned to	
IP Address	192.168.40.153		
Host name			

Import Visual Workflows

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

1. Click the (**Menu**) button.
2. Navigate to **Workflow > Configurator**.
3. Click the (**Import**) button in the Command bar.

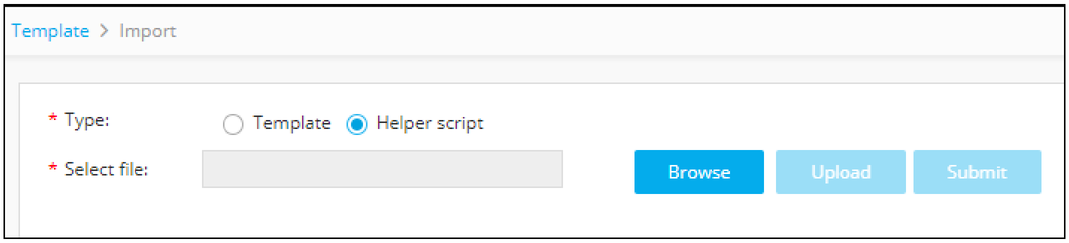


4. On the *Import* screen that opens, complete the following steps:
   a. Click the **Browse** button.
   b. Select the zip file containing one or more workflows, then click **Upload**.
   c. In the table at the bottom of the Import page, select the check box beside the unzipped workflow file.
   d. Click **Submit** to deploy the workflow into your AppViewX environment.

Import Helper Scripts

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

1. Click the ☰ (**Menu**) button.
2. Navigate to **Provisioning > Templates**.
3. Click the ⤓ (**Import**) button in the Command bar.
4. On the *Import* screen that opens, complete the following steps:
   a. Select the **Helper script** radio button.
   b. Click **Browse** and select the helper script zip file you want to import.
   c. Click **Upload** to import the file and view its contents.



* Type: ○ Template ● Helper script

   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.

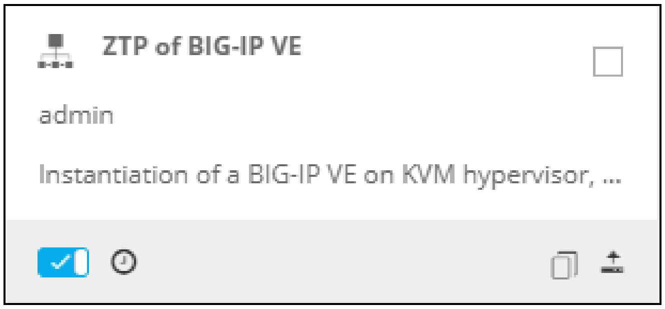
Enable a Workflow

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

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

   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.



ZTP of BIG-IP VE

admin

Instantiation of a BIG-IP VE on KVM hypervisor, ...

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 ▶ (**Run workflow**) button on the ZTP of BIG-IP VE workflow.
4. On the *Form Builder* screen that opens, click the **Get Host Machine** button to retrieve the list of host machines.
5. From the **Select Host Machine** dropdown list, select the host machine for which you want to create a guest Virtual Machine (VM).
6. In the **VM Name** field, enter a name to help the users identify it.
7. In the **Use BIG-IP Flavours** field, select how you want to configure the guest VM:
   a. Select **Yes** to use the BIG-IP Flavour configurations that are provided by F5.
   b. Select **No** to manually enter the CPU Cores and RAM size of the guest VM.
8. Click the **Get Management Interface** button to retrieve the list of interfaces available in the host machine.
9. From the **Management Interface** dropdown list, select the interface you want to use for configuration and management operations.
10. 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 which are used for management operations.
11. 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 in this workflow.
12. 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 a registration license key you received from F5 in order to communicate with the device.

   b. Enter the details (such as name, job title, company name, address, phone number, email address, host name, password, and time zone) in order to get the license from F5.

13. If you want to use a BIG-IQ device for licensing, select **Yes** and do the following:
    a. Click the **Get BIG-IQ device** button to retrieve the list of BIG-IQ devices. Select the BIG-IQ device you want to use for licensing from the dropdown list.
    b. Click the **Get Available BIG-IQ Device Pools** to retrieve the list of pools available in the BIG-IQ device. Select the pool you want to use from the **BIG-IQ Device Pool** dropdown list.
    c. Click the **Get RegKey Pools** button to retrieve the list of registration key pools available in the BIG-IQ device. Select the license key pool you want to use from the **Registration Key Pool** dropdown list.
    d. Enter the details (such as host name, password, and time zone) in order to get the license from BIG-IQ.
14. From the **Provisioning Modules** dropdown list, select the modules you want to be provisioned.

    Note: This option will appear only when you manually enter the configuration details of the guest VM.
15. Click the **Get IPAM Devices** button to retrieve the list of Infoblox devices present in the AppViewX inventory.
16. Select the Infoblox 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.
17. In the **Vlan name** field, enter a name for the VLAN connection to help users identify it.
18. Click the **Get NTP Servers** button to retrieve the list of NTP servers present in the AppViewX inventory.
19. Select the NTP server you want to use for time synchronization from the dropdown list.
20. Click the **Get DNS Name Servers** button to retrieve the list of DNS name servers present in the AppViewX inventory.
21. Select the DNS server you want to use for DNS resolution from the dropdown list.
22. 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.
23. 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.

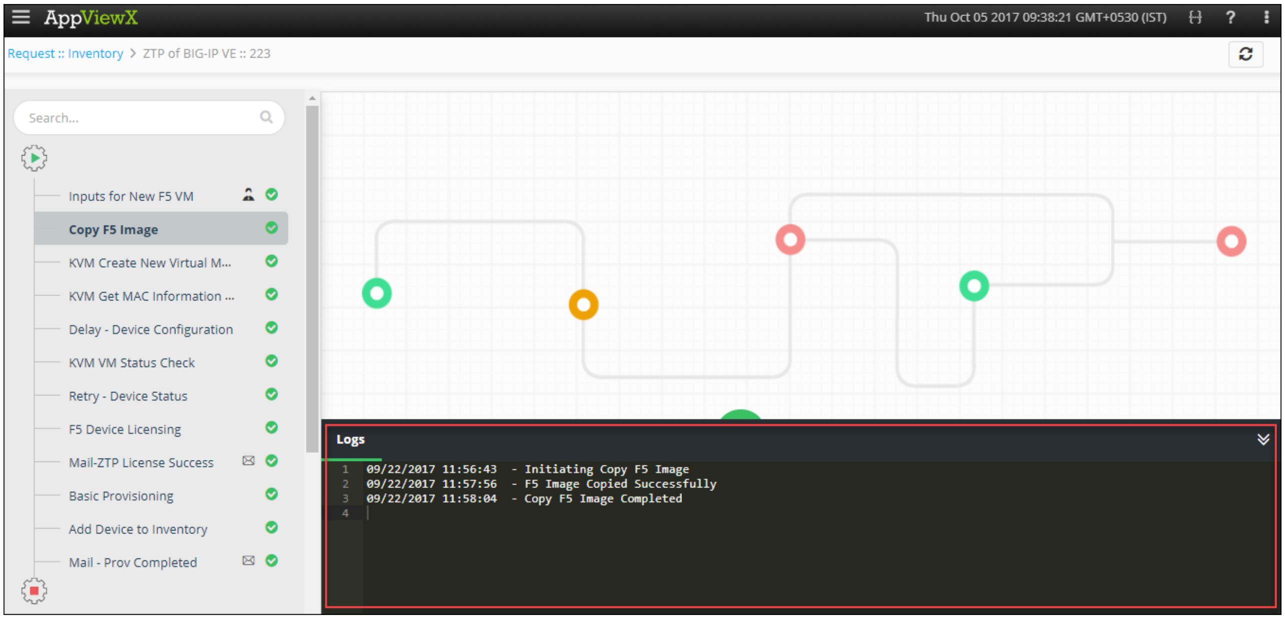
24. In the **Device Name for AVX Inventory field**, enter a name for the device. The device name should be same as how it is mentioned in the AppViewX inventory.
25. Depending on whether or not you want to integrate **ServiceNow** (SNOW), select the **Yes** or **No** radio button. To integrate the ITSM tool, you must enter the following details:
    a. Schedule the service window time and date using the **Start Date** and **End Date** fields. Click the 📅 (**Calendar**) button to select the start and end date respectively. The configuration changes will be implemented during this service window.
26. Click the **Create ServiceNow Ticket** button to retrieve the ticket number. A new request ID will auto-filled in the **Ticket Number** field.
27. From the **Business Unit** dropdown list, select the business unit from where you want the workflow to be triggered.
28. In the **Mail ID** field, enter an email address of the recipient to whom you want to send the status of the workflow.
29. Click **Submit**.

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

WorkOrder 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.



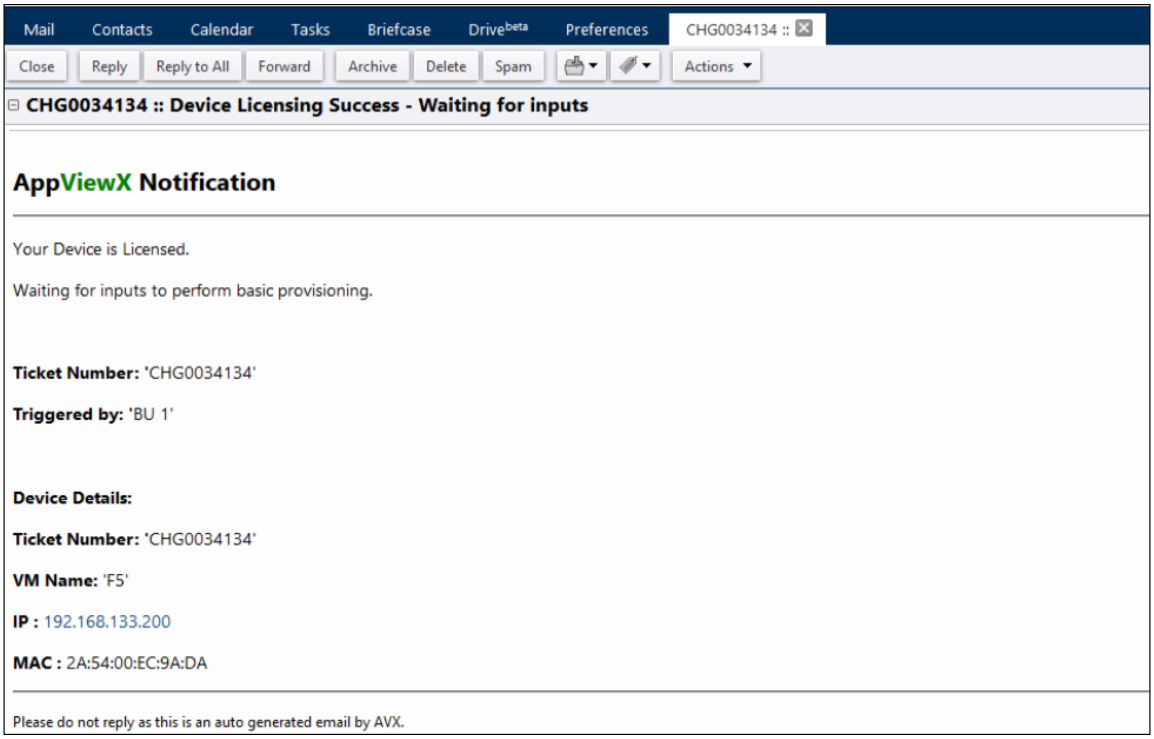
```
09/22/2017 11:56:43  - Initiating Copy F5 Image
09/22/2017 11:57:56  - F5 Image Copied Successfully
09/22/2017 11:58:04  - Copy F5 Image Completed
```

1. **Copy F5 Image —** an image (**qcow2** format) will be copied from the KVM home directory to the storage pool **/opt/vm**
2. **KVM Create New Virtual Machine —** a new VM will be created based on the inputs provided in the form builder.

3. **KVM Get MAC Information of the VM –** running the commands on the host will provide MAC information of the guest VM.
4. **Delay Device Configuration –** a delay of 1 minute is added in order to give time for the VM configuration. It is also based on the speed of KVM, if the KVM is already loaded then the delay time will vary.
5. **KVM VM Status Check –** the KVM VM status check will ensure that the device is up and running. The IP address of the guest VM will be obtained.
6. **F5 Device Licensing**

   If the user selected BYOL, the license key will be communicated to the device to get the dossier key. This dossier key will be sent to *activate.f5.com*, which will return the license. Then, the license will be pushed to the device and activated.

   If the user selected BIG-IQ, the free license available from the license key pool will be obtained for licensing. The new BIG-IP VE will be added to the BIG-IQ device as a managed entity and the license from the selected key pool will be provided to the device.
7. **Mail-ZTP License Success –** an email notification on the status of the BIG-IP VE licensing will be triggered to the users.



CHG0034134 :: Device Licensing Success - Waiting for inputs

AppViewX Notification

Your Device is Licensed.

Waiting for inputs to perform basic provisioning.

Ticket Number: 'CHG0034134'

Triggered by: 'BU 1'

Device Details:

Ticket Number: 'CHG0034134'

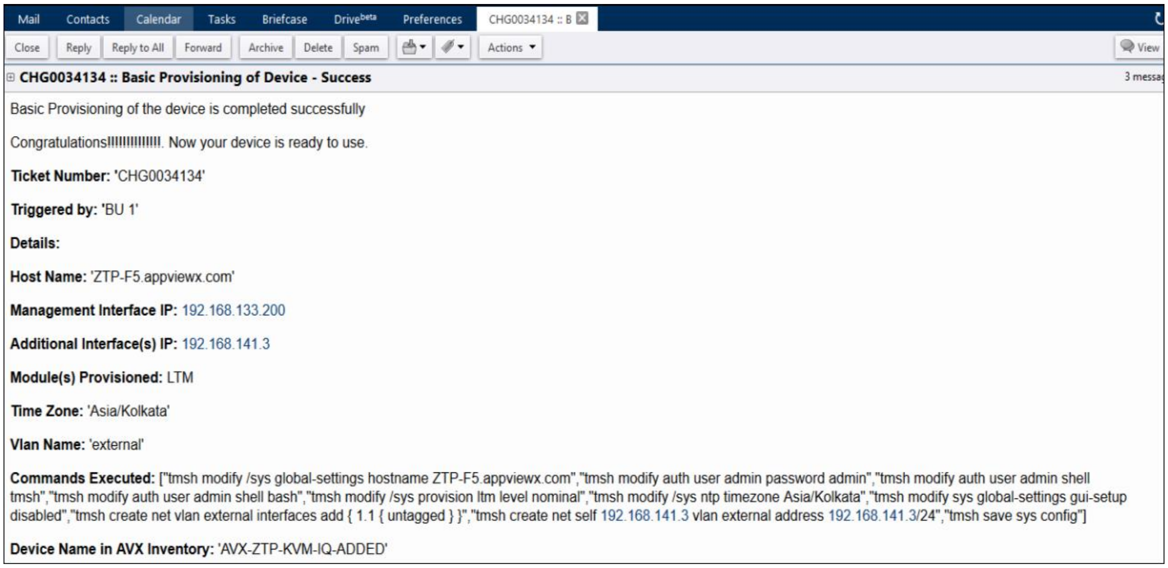
VM Name: 'F5'

IP : 192.168.133.200

MAC : 2A:54:00:EC:9A:DA

Please do not reply as this is an auto generated email by AVX.

8. **Basic Provisioning –** the BIG-IP VE will be provisioned for external network handling based on the details provided in the form builder.
9. **Add Device to Inventory –** add the BIG-IP VE to the AppViewX ADC device inventory.
10. **Mail - Prov Completed –** an email notification on the status and details of the BIG-IP VE provisioning will be triggered to the users.



CHG0034134 :: Basic Provisioning of Device - Success

Basic Provisioning of the device is completed successfully

Congratulations!!!!!!!!!!!!!. Now your device is ready to use.

Ticket Number: 'CHG0034134'

Triggered by: 'BU 1'

Details:

Host Name: 'ZTP-F5.appviewx.com'

Management Interface IP: 192.168.133.200

Additional Interface(s) IP: 192.168.141.3

Module(s) Provisioned: LTM

Time Zone: 'Asia/Kolkata'

Vlan Name: 'external'

Commands Executed: ["tmsh modify /sys global-settings hostname ZTP-F5.appviewx.com","tmsh modify auth user admin password admin","tmsh modify auth user admin shell tmsh","tmsh modify auth user admin shell bash","tmsh modify /sys provision ltm level nominal","tmsh modify /sys ntp timezone Asia/Kolkata","tmsh modify sys global-settings gui-setup disabled","tmsh create net vlan external interfaces add { 1.1 { untagged } }","tmsh create net self 192.168.141.3 vlan external address 192.168.141.3/24","tmsh save sys config"]

Device Name in AVX Inventory: 'AVX-ZTP-KVM-IQ-ADDED'

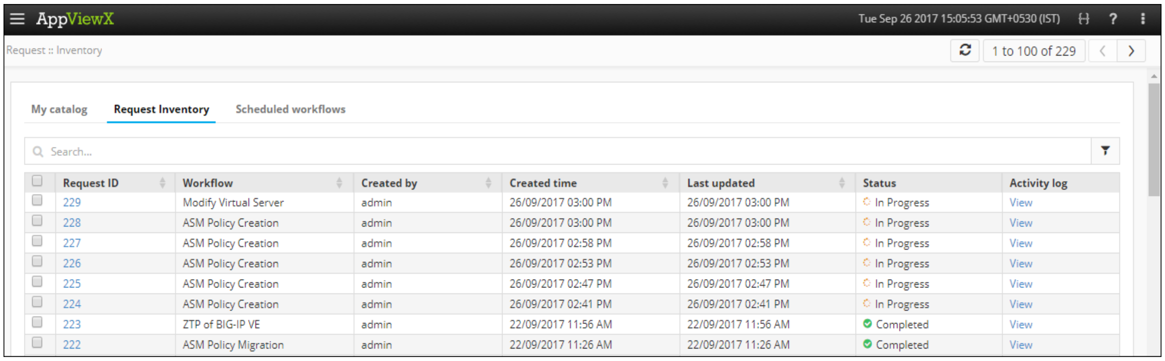
Request Inventory

To go to Request inventory, complete the following steps:

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

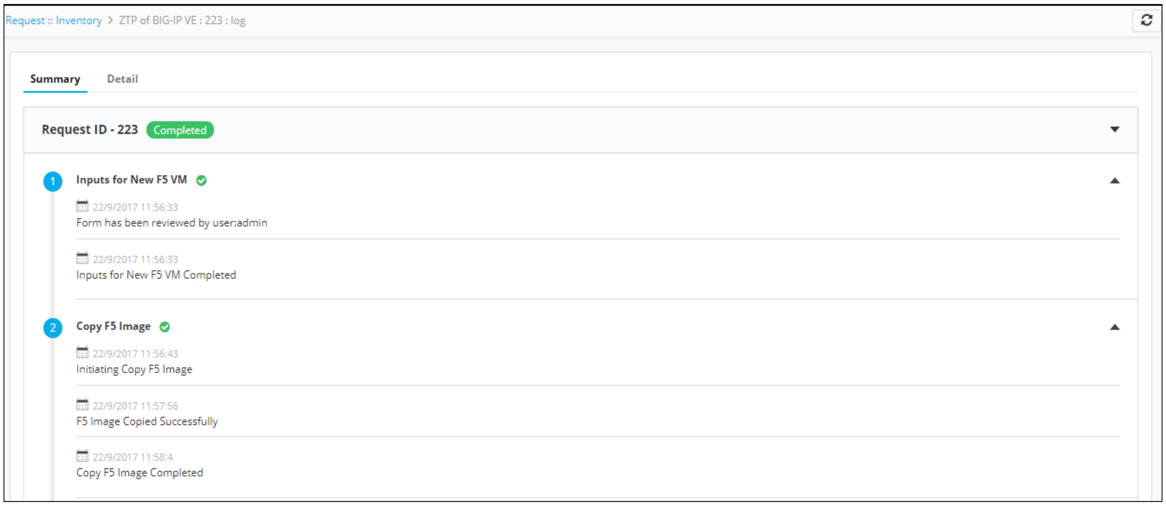
   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the **Request Inventory** tab.

   This displays all workflows that have been triggered. On the **Request Inventory** screen, you can perform the following tasks: Search for a request using the **Search** field. Click the ▼ (**Filter**) button to select the options you want to use to sort the requests.



☐	Request ID	Workflow	Created by	Created time	Last updated	Status	Activity log
☐	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** created for ZTP of BIG-IP VE in order to view the tasks or phases of a request in a tree-view. For more details, refer to the (WorkOrder flow) section of this guide
5. You can also view the following details of the request that 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.



Request ID - 223 Completed

1 Inputs for New F5 VM ✓

22/9/2017 11:56:33
Form has been reviewed by user:admin

22/9/2017 11:56:33
Inputs for New F5 VM Completed

2 Copy F5 Image ✓

22/9/2017 11:56:43
Initiating Copy F5 Image

22/9/2017 11:57:56
F5 Image Copied Successfully

22/9/2017 11:58:4
Copy F5 Image Completed

Schedule a Workflows

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 here.
5. Click **Save**.

Scheduled workflows

Displays all workflows that have been scheduled. 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:
   a. In the **View log** column, click **View** to display the details of a scheduled workflow.
   b. 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 fails?

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 ServiceNow ticket.