appviewx

ADC+ Admin Guide

Version: 2022.1.0

Copyright AppViewX, Inc.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2022.1.0 FP2.	December 2022

About the Documentation

This guide explains the procedures for setting up and managing ADC+ administrative functionality.

Documentation Conventions

This section defines the Notice icon and text convention used in this guide.

Notice Icons

Convention	Description
Note	Indicates readers to take note. Notes contain helpful suggestions or references to material not covered in the document.
Tip	Indicates readers that they can save time by performing the action described in the paragraph affixed to this icon.
Warning	Indicates readers that they can save time by performing the action described in the paragraph affixed to this icon.
Best Practice	Alerts readers to a recommended use or implementation.

Audience

This document is intended for,

- Application teams
- Network Operations (NetOps)
- NetDevOps
- Traffic Management
- Automation and DevOps

Chapter 1: Getting Started

Overview

Use this guide to set up and manage ADC+ administrative functionality. Also learn about the new features and capabilities that make it easier for you to configure and administer your ADC+ deployment. Setup of the AppViewX Cloud Connector is necessary to enable the connectivity between AppViewX Cloud and the Enterprise Network. For AppViewX SaaS deployment, refer to AppViewX Cloud Connector User Guide. The documents helps to configure below functionalities:

- AppViewX provides App centric visibility of your ADC infrastructure in a single window.
- Onboard the supported ADC vendor devices (Hardware, Cloud and Software) into the AppViewX inventory using the IP Address/FQDN.
- Helps to configure credentials and Discover the Applications/Objects along with its configuration that are hosted on the devices. The Discovered Applications can be accessed within the product.
- Steps to configure the access control policies to access devices and its application objects. The AppViewX Platform applies granular access control to application objects, certificates and configuration templates.
- Explains possible Search engine patterns that allows to look for any application and also visualize the topological view starting from the Global load balancer to the end server. This provides the network teams visibility into the infrastructure to troubleshoot application-related issues faster.
- Steps to configure dashboard to monitor Application health, state, status, utilization and performance through pre built dashboards. Monitor and Manage Application Traffic through Custom Dashboards and Widgets that allows Traffic routing, Monitor live traffic and Distributes traffic ratio across data centers.
- Steps to manage network configuration by automating the backups, track and report network changes and ensure they are compliant with the defined policies.
- Helps to understand/configure the Settings to periodically monitor your Application Services or Devices to get notified of any critical changes via alerting module.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	
Chrome	Till latest (Version 80.0)	
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Device	OS	Resolution
Desktop	Windows	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Linux	1024 X 768 onwards, 1366x768, 1920x1080, Higher
Desktop	Mac	1024 X 768 onwards, 1366x768, 1920x1080, Higher
iPad	iOS	1024 X 768

Chapter 2: Discover/Onboard an ADC Device

Discover/Onboard an ADC Device

Onboard the supported ADC vendor devices (Hardware, Cloud, and Software) into the AppViewX inventory using the IP Address/FQDN. AppViewX will initiate the communication using the provided credentials and Discover the Applications/Objects along with their configuration that are hosted on the devices. The Discovered Applications can be accessed within the product.

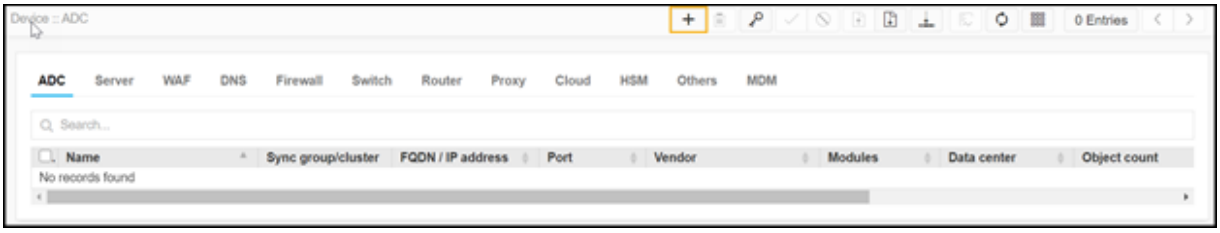
After navigating to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**, you can also add devices under the DNS, WAF, or Others tab. Under the following tabs,

- **DNS** - add a device to integrate it with the DNS and this integration can be used in the ADC automation workflow.
- **Others** - add Bluecat, infoblox, etc., devices and used in ADC automation workflow.
- **WAF** - add a device to identify the vulnerability for the device using ADC automation workflow.

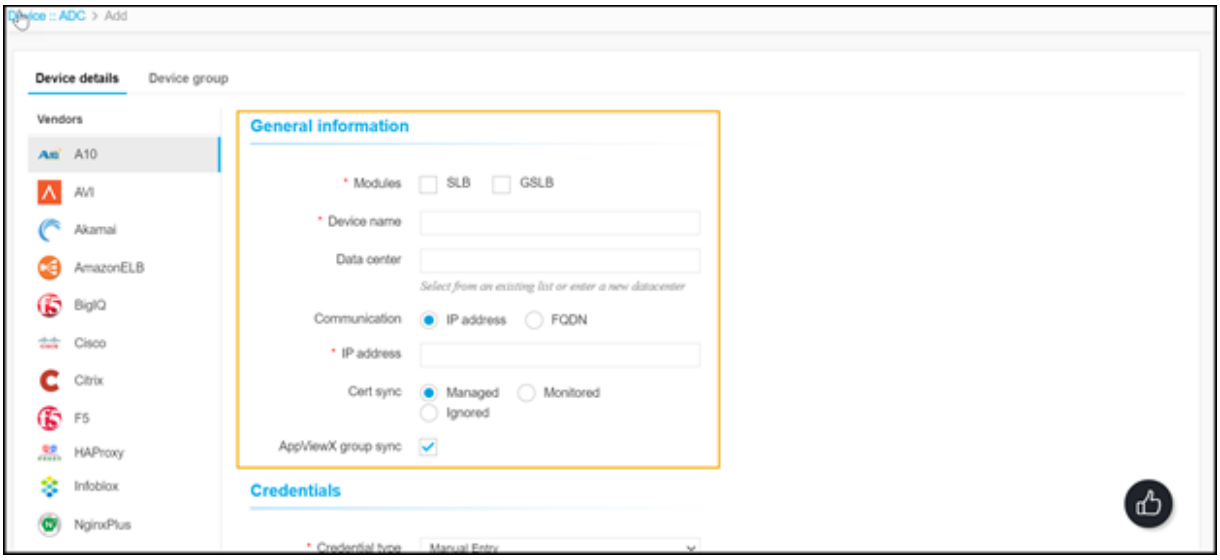
For vendor-specific device addition, refer to Discover/Onboard ADC Device for Vendor.

To onboard a device into Device Inventory,

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. In the **ADC** tab, click add + button located upper right corner.



   The **Add** page appears.
3. Enter or select the field information in the **General Information** section.



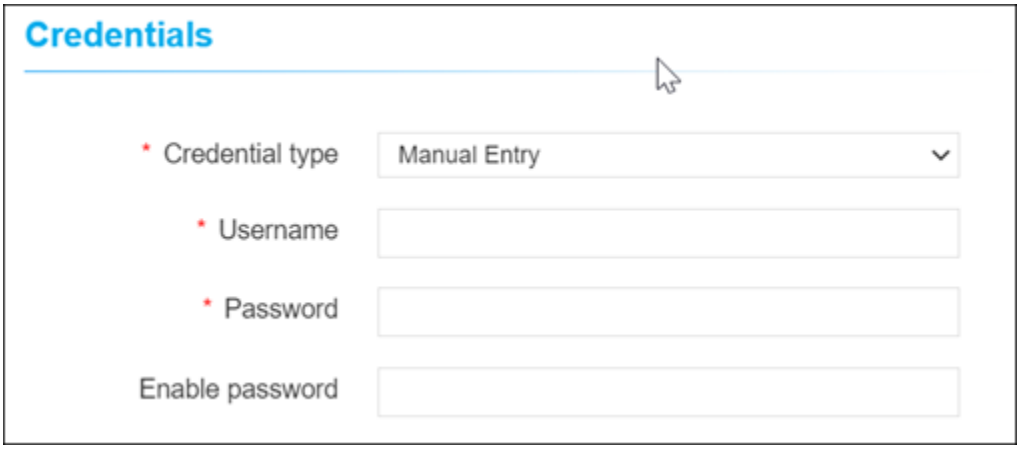
The following table provides the field description for adding ADC device details in the **General Information** page:

Field	Description
***Modules**	Select one of the following or both for ADC device in AppViewX: • **GSLB** - Global Server Load Balancing is the process of distributing application traffic among a large number of connected servers available across the world at multiple geographic locations. • **SLB** - Server load balancing distributes traffic locally from GSLBs to appropriate servers to ensure consistent, high-performance application delivery. Based on this module selection, the respective configuration of the device will be fetched into AppViewX.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that ADC devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the ADC device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is

Field	Description
	resolved to more than one device IP, AppViewX will choose a random IP for communication. • **Port** - A custom-enabled port of the Device, through which the communication will happen from AppViewX.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Cert sync	Provision to discover and manage the SSL certificates from the ADC devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the ADC device.
AppViewX group sync	Select this checkbox to enable the group sync. AppViewX Group Sync ensures configurations are in sync between active/primary and secondary/failover devices. This sync interval can be configured at AppViewX's System Settings page.

Note: The asterisk (*) symbol indicates mandatory fields.

4. Enter or select the field information in the **Credentials** section:

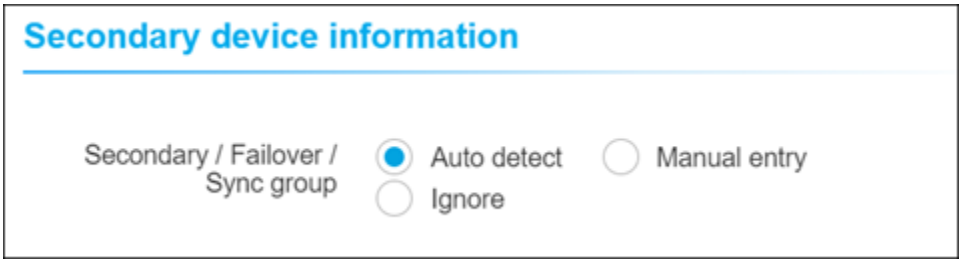


The following table provides the field description for adding ADC device details in the **Credentials** page:

Field	Description
***Credential type**	Credentials can be manually provided or stored as a one-time entry onto the credential library and referred at the time of device addition. Select one of the following credential types from the drop-down list: • **Manual Entry** - The user name and password of the device need to be entered with device details. By default, the Manual Entry option is selected. • **AppViewX Credential List** - The user name and password can be added to the List and that entry can be referred to during device addition. The credential lists are integrated within AppViewX application for the secured authentication. The available credential lists are: • AppViewX • CyberArk • Thycotic Secret • HashiCorp To create a credential list, see Creating Credential List in the *Platform User Guide*.
***Username**	Username for the ADC device when you select the **Manual Entry** credential type.
***Password**	Valid password for the ADC device when you select the **Manual Entry** credential type. **Note:** Use strong passwords for secure device communication. Your Passwords can be of any length with a combination of alpha-numerical, symbols, and special characters.
Enable password	For the **AppViewX Credential List** credential type, select your credential list with a CYBERARK username and app ID from the dropdown list.

Note: The asterisk (*) symbol indicates mandatory fields.

5. Enter or select the field information in the **Secondary device information** section as follows:



- **Auto-Detect** - This option will automatically detect the corresponding secondary devices and add it as a new entry into AppViewX inventory using the Primary device's credential.
- **Manual Entry** - This selection will enable you to manually add Secondary devices with a Sync-group name entered for reference. This name will be used to identify the pairs in the inventory. Follow similar steps.
- **Ignore** - This option can be enabled if you need to ignore the detection of the secondary device associated with the current device.

Note:

- In a typical network configuration, Application traffic will be handled by multiple ADC devices for ensuring the high availability of the application. This distribution of ADC servers will be meaningful during any disaster recovery and avoid a single point of failure. To achieve this, multiple ADC devices will be configured in Active/Standby or in failover groups. In this grouping, one ADC device will be serving the traffic and the rest of the devices in the group will act as a backup in case of a failure. The configuration will be in sync between these devices. At the same time, devices in a sync group can be in active-active mode also. You can manage one or more such Secondary devices (Failover/Standby devices) in inventory.
- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

6. Click the **Save** button to add an ADC device.

Note:

- To discard the changes, click the Cancel button. Note: Repeat the same steps to add more ADC device(s).
- Repeatt tthe same stteps tto add morre ADC devviice(s).

• Discover/Onboard an ADC Device
• Vendor Specific Discover/Onboard ADC Device

Vendor Specific Discover/Onboard ADC Device

- A10
- AVI
- Akamai
- Amazon ELB
- BigIQ
- Cisco
- Citrix
- F5
- HAProxy
- InfoBlox
- NginxPlus

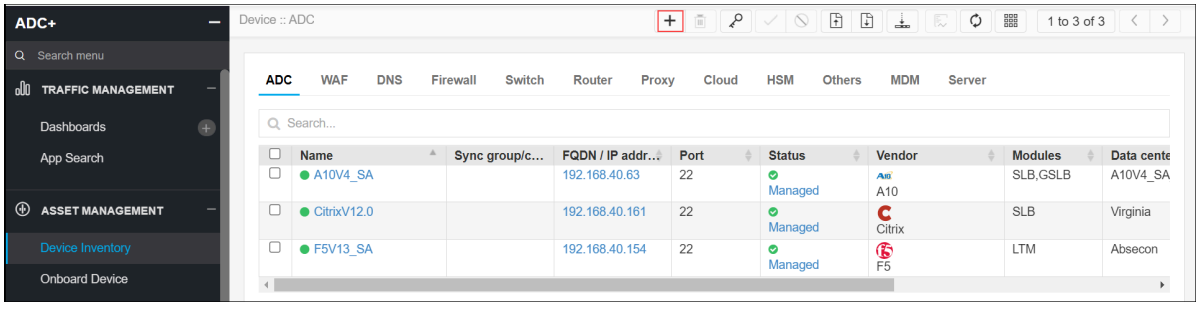
A10

- Adding A10 Device
- Validating the A10 device addition

Adding A10 Device

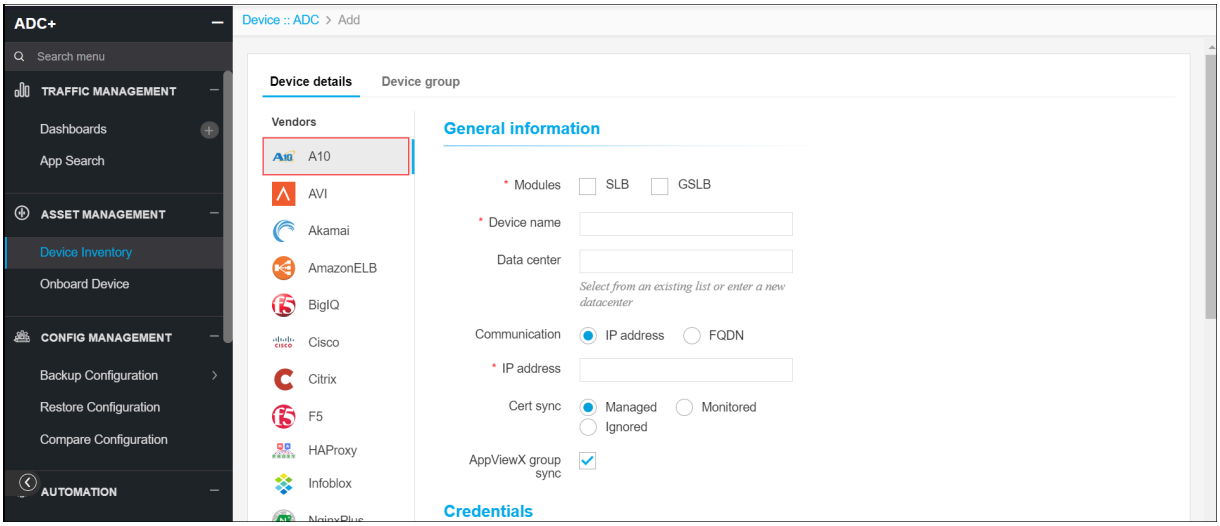
To add A10 device,

1. Log in to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

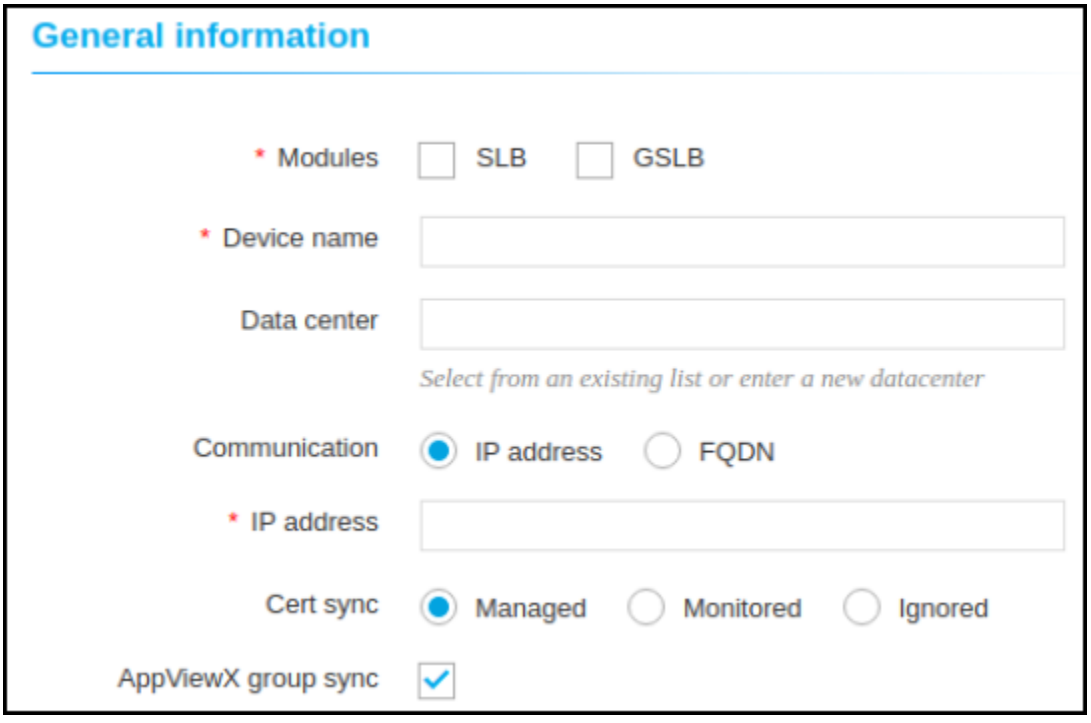


- Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **A10** from the left sidebar.



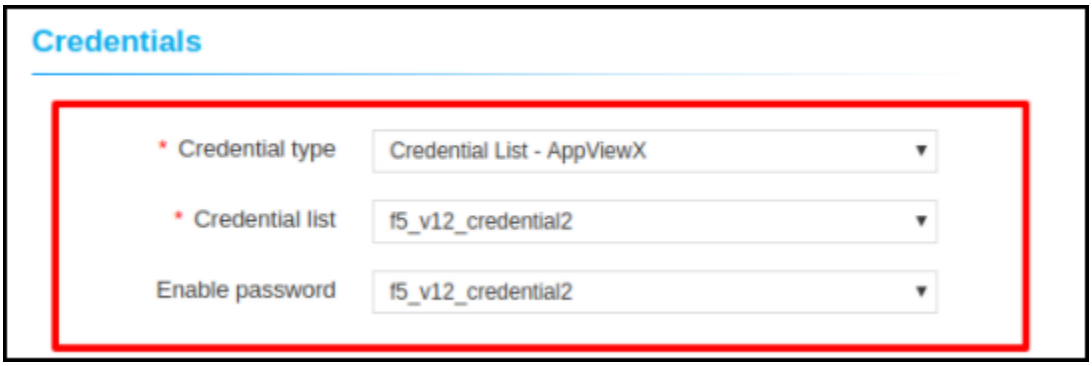
5. Enter or select the field information in the **General information** section.



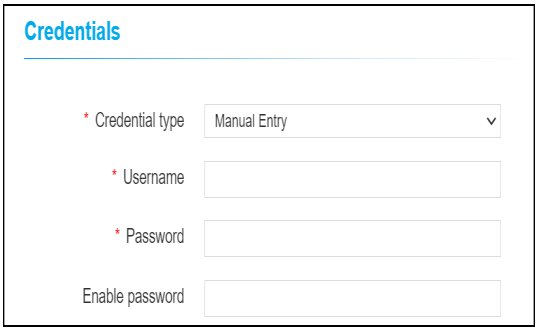
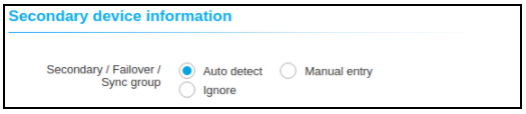
6. The following table provides the field description for adding ADC device details in the **General information** section:

Name	Type	Mandatory	Description	Validation
Module	Check box	Yes	SLB / GSLB Module.	NA
Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Communication	Radio button	Yes	Devices can be accessed using an IP address or FQDN.	NA
IP Address	Text	Yes	The ipv4 address of the device.	The IP address should be in the right format.
FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.
Cert Sync	Radio button	Yes	Managed: The certificates of the device can be managed. Monitored: The certificates of the device can be monitored. Ignored: The certificate sync can be ignored.	NA
AppViewX Group Sync	Check box	No	This should be enabled if the user wants to sync the devices within the device group.	NA

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credential List**.

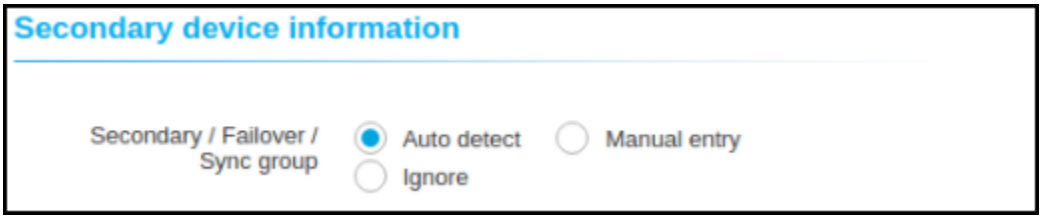


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
Credential type	Dropdown	Yes	Manual entry: The user should enter the username and password.  Credential List: The user can select the credential details which are already stored in the credential inventory page. 	NA

Name	Type	Mandatory	Description	Validation
Username	Text	Yes	If manual entry is selected, the user name should be entered by the user.	NA
Password	Text	Yes	If manual entry is selected, the password should be entered by the user.	NA
Enable password	Text	No	Enable password of the A10 device.	NA

9. Enter or select the field information in the **Secondary device information** section.



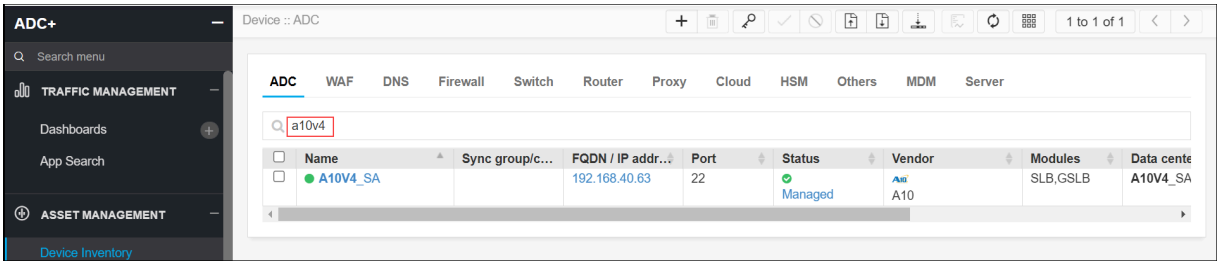
10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

11. Click **Save**.

Validating the A10 device addition

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



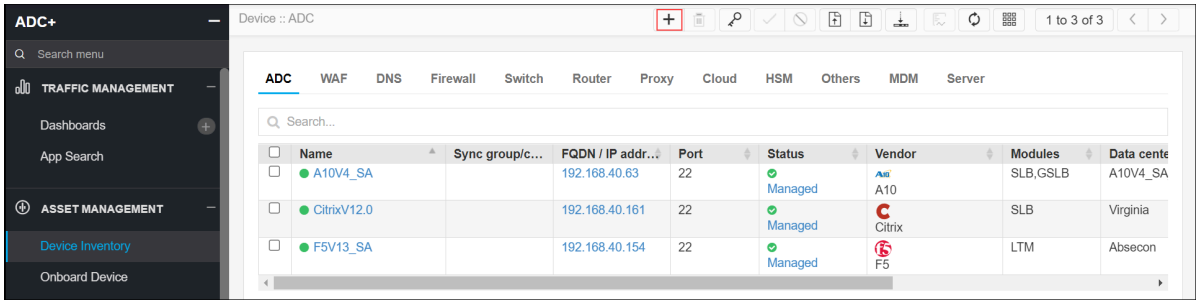
AVI

- Adding AVI Device
- Validating the AVI Device Addition

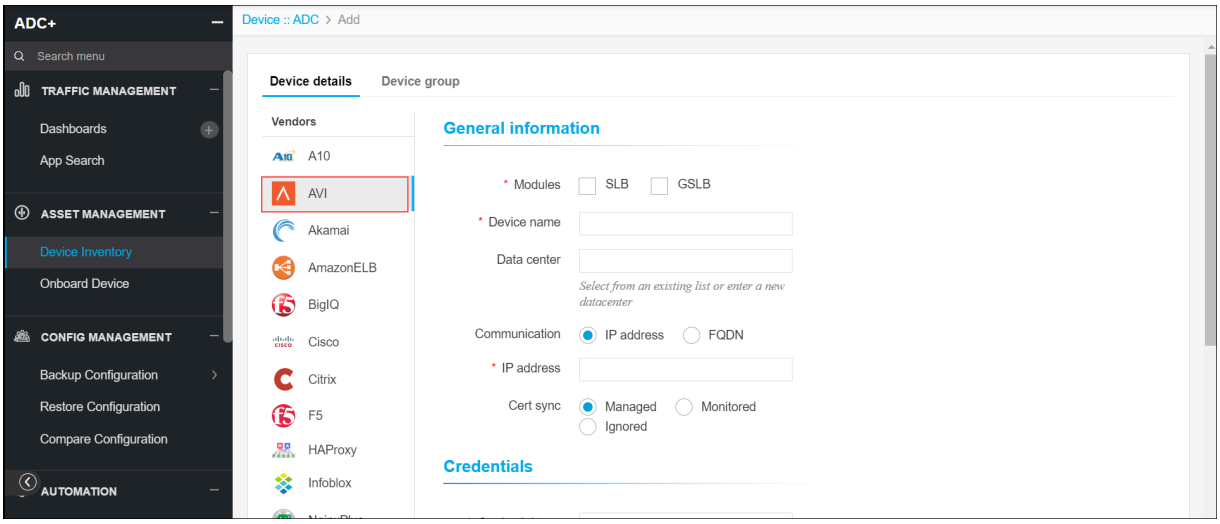
Adding AVI Device

To add AVI device,

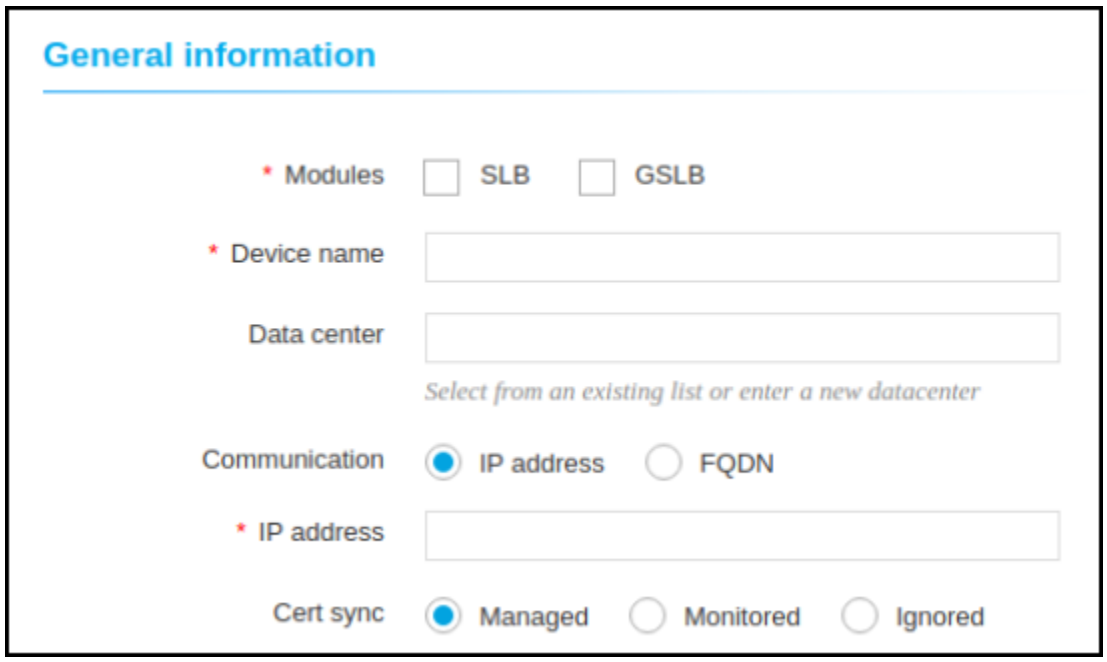
1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - Click **Onboard Device** in the left navigation panel.
4. In the **Device details** page, select **AVI** from the left sidebar.



5. Enter or select the field information in the **General information** section.

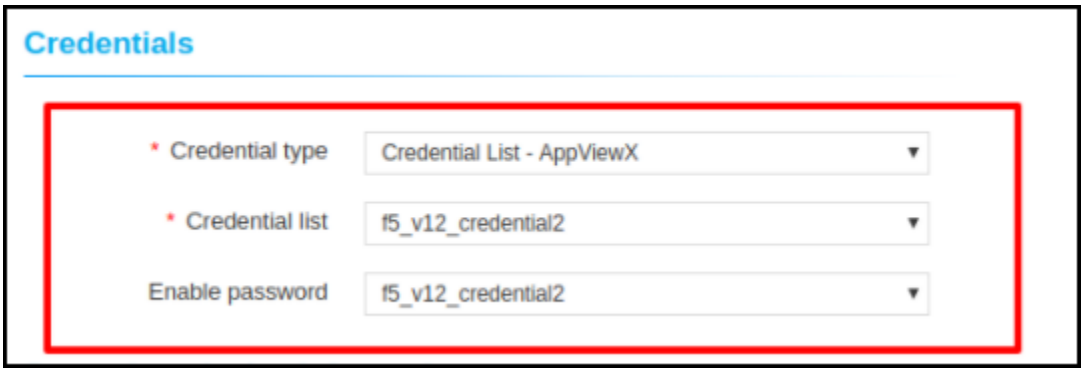


6. The following table provides the field description for adding ADC device details in the **General information** section:

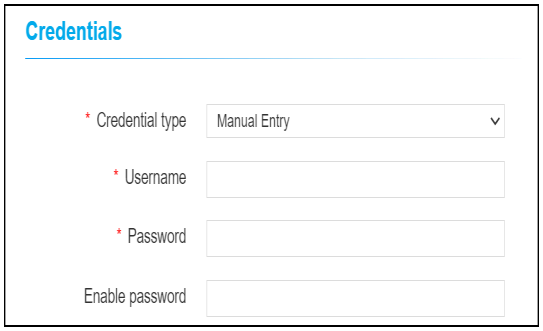
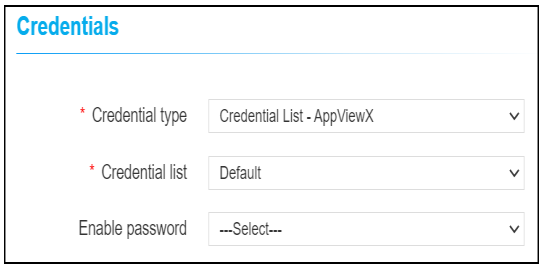
Name	Type	Mandatory	Description	Validation
Module	Check box	Yes	SLB / GSLB Module.	NA

Name	Type	Mandatory	Description	Validation
Device name	Text	Yes	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Communication	Radio button	Yes	Devices can be accessed using an IP address or FQDN.	NA
IP Address	Text	Yes	The ipv4 address of the device.	The IP address should be in the right format.
FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.
Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA

7. Enter or select the field information in the **Credentials** section.

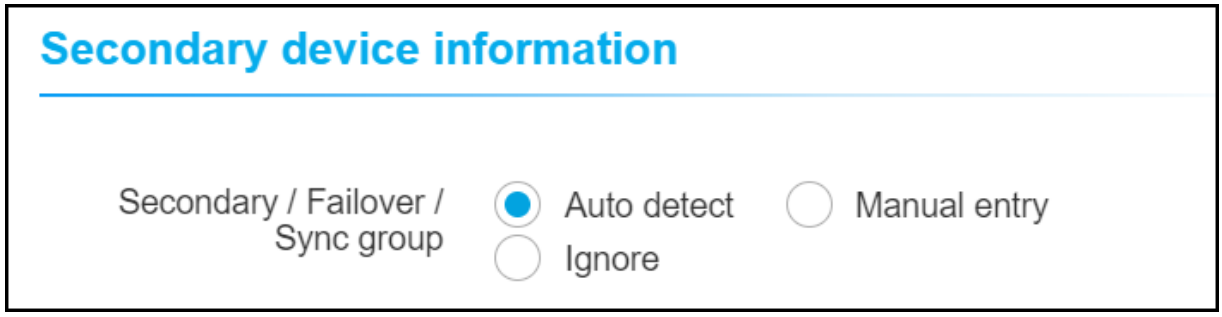


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	NA

Name	Type	Mandatory	Description	Validation
Username	Text	Yes	If manual entry is selected, the user name should be entered by the user.	NA
Password	Text	Yes	If manual entry is selected, the password should be entered by the user.	NA
Enable password	Text	No	Enable password of the A10 device.	NA

9. Enter or select the field information in the Secondary device information section.



10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

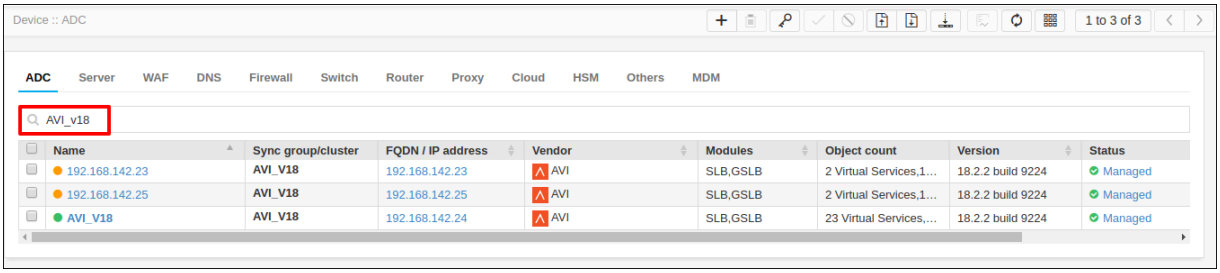
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

11. Click **Save**.

Validating the AVI Device Addition

After adding the device, you can validate the device by searching the device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



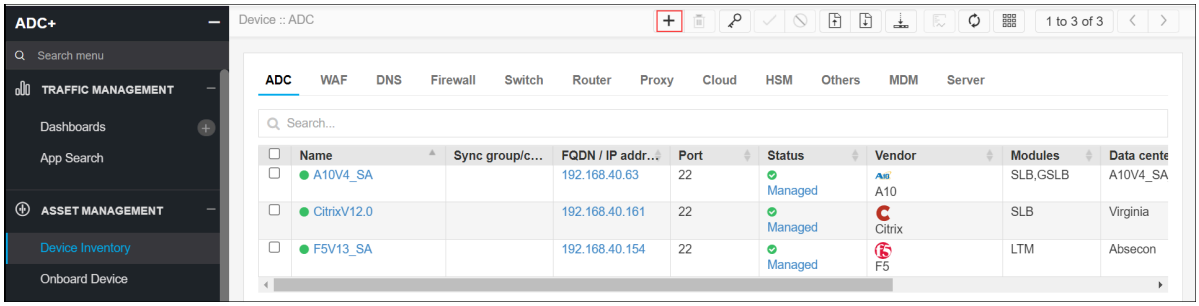
Akamai

- Adding Akamai Device
- Validating the Akamai Device Addition

Adding Akamai Device

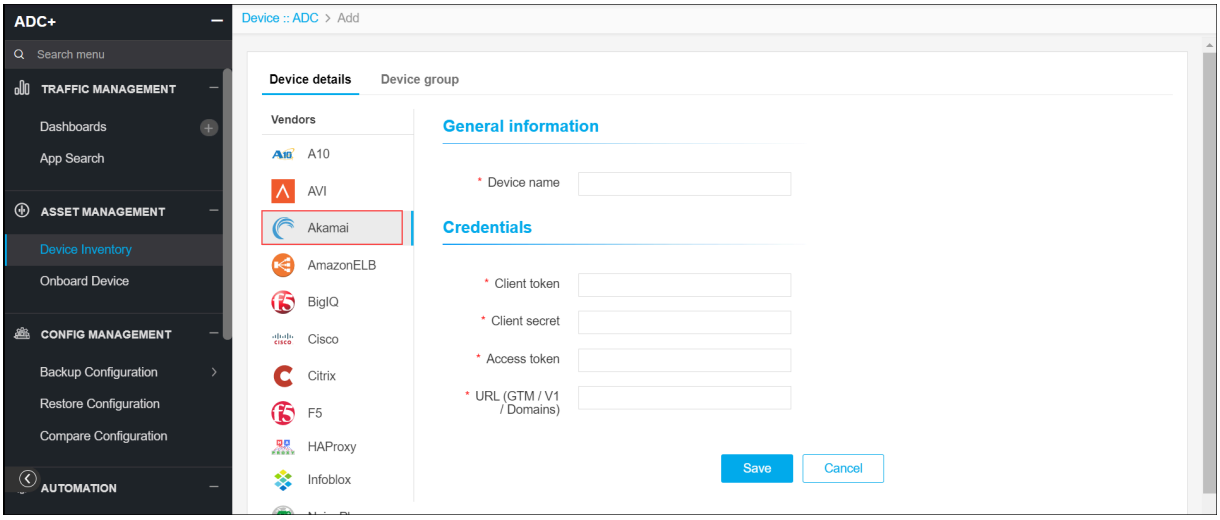
To add Akamai device,

1. Log in to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **Akamai** from the left sidebar.



5. Enter the required details for the device addition.

Name	Type	Mandatory	Description	Validation
*Device name	Text	Yes	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
*Client token	Text	Yes	Client token of the Akamai device.	NA
*Client secret	Text	Yes	Client secret of the Akamai device.	NA
*Access token	Text	Yes	Access token of the device.	NA
*URL	Text	Yes	Valid URL of the Akamai device.	NA

6. Click **Save**.

Validating the Akamai Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.

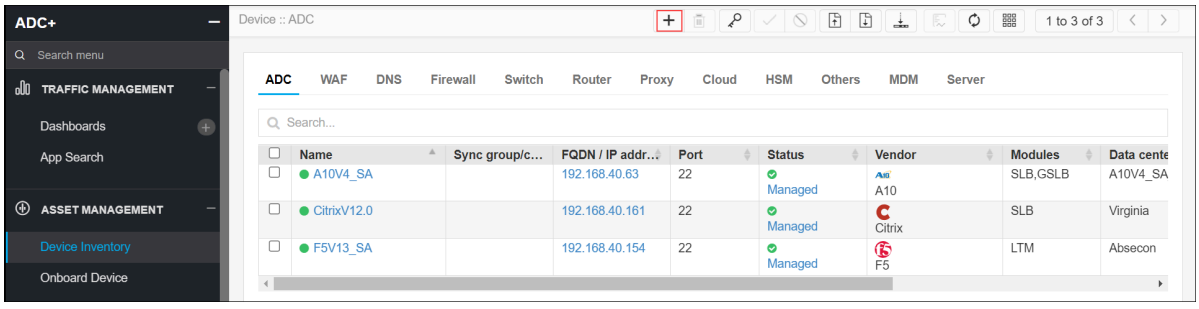
Amazon ELB

- Adding Amazon ELB
- Validating the Amazon ELB Device Addition

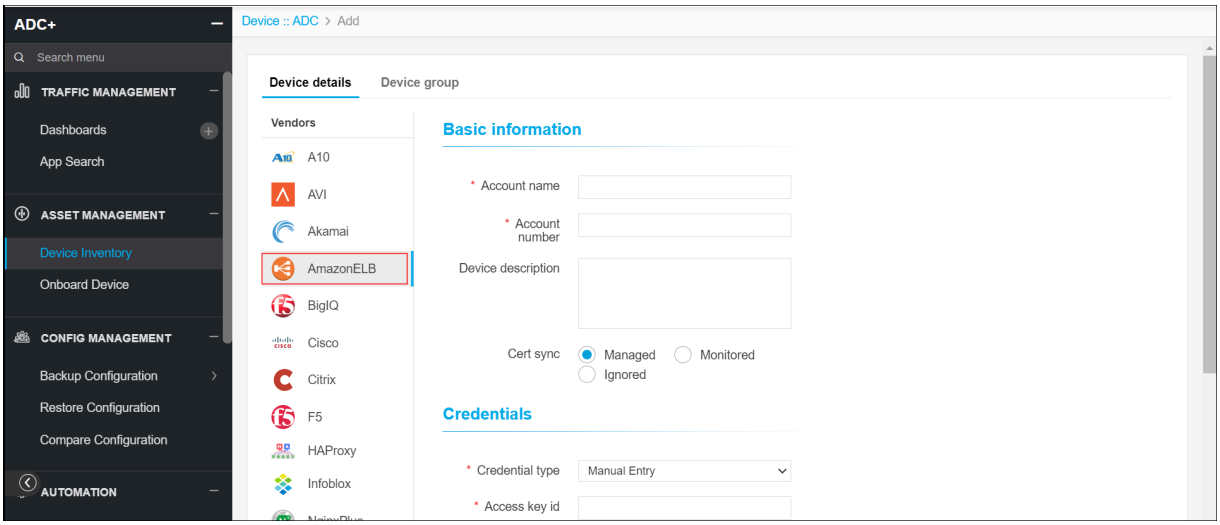
Adding Amazon ELB

To add Amazon ELB,

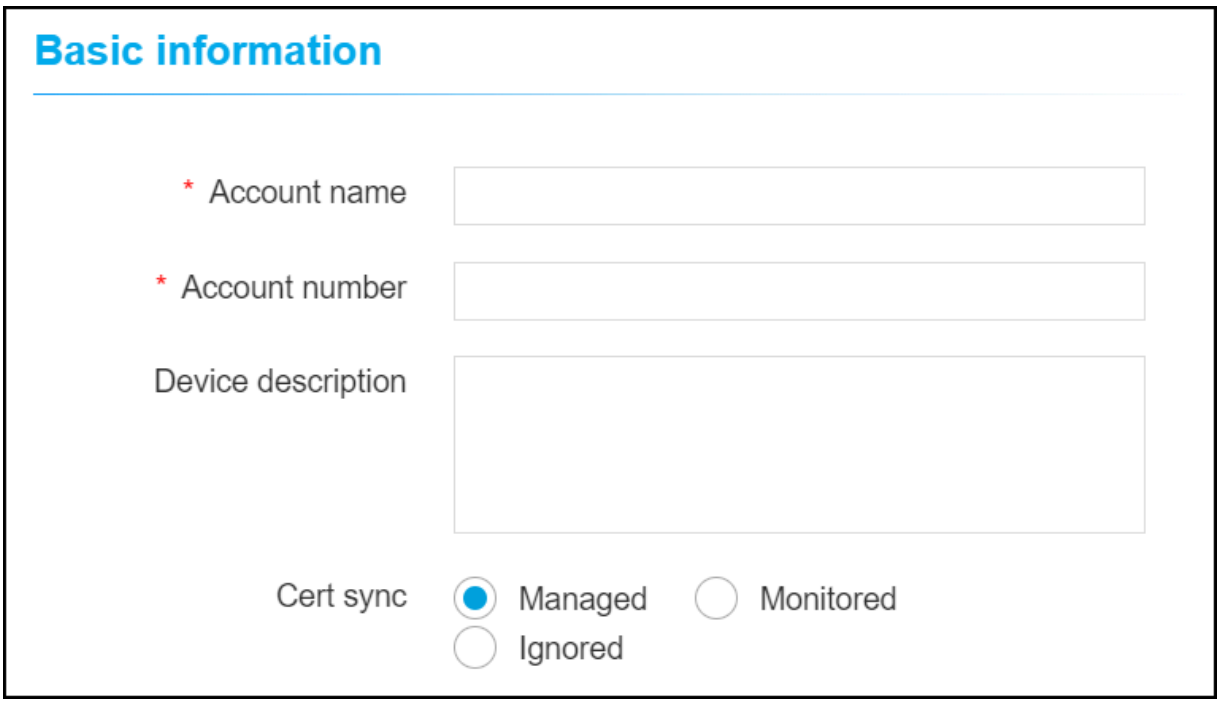
1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - Click **Onboard Device** in the left navigation panel.
4. In the **Device details** page, select Amazon ELB from the left sidebar.



5. Enter or select the field information in the **Basic information** section.

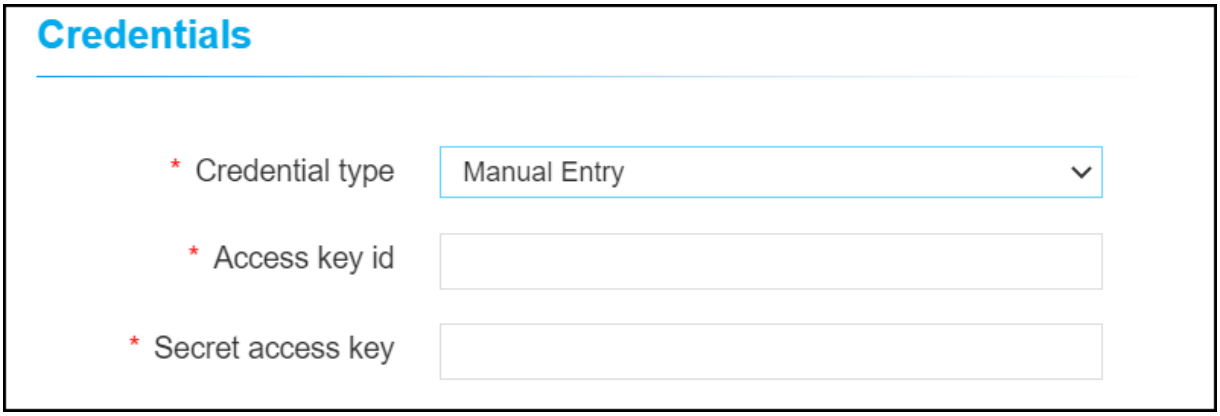


6. The following table provides the field description for adding ADC device details in the **Basic information** section:

Name	Type	Mandatory	Description	Validation
Account name	Text	Yes	The account name of the AmazonELB device.	NA

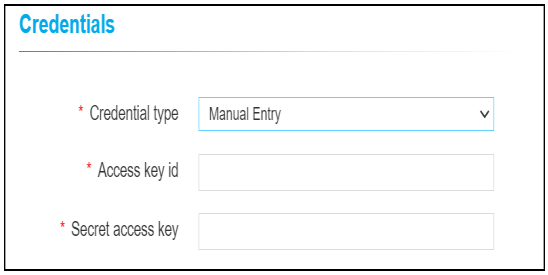
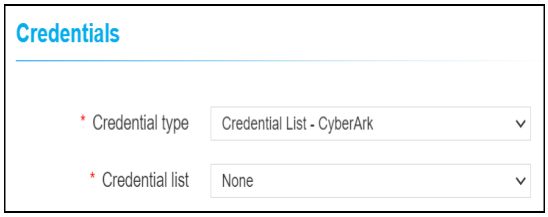
Name	Type	Mandatory	Description	Validation
Account number	Text	Yes	Account number of the AmazonEB device.	Numbers only.
Device description	Text	No	Description about the AmazonELB account.	NA
Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

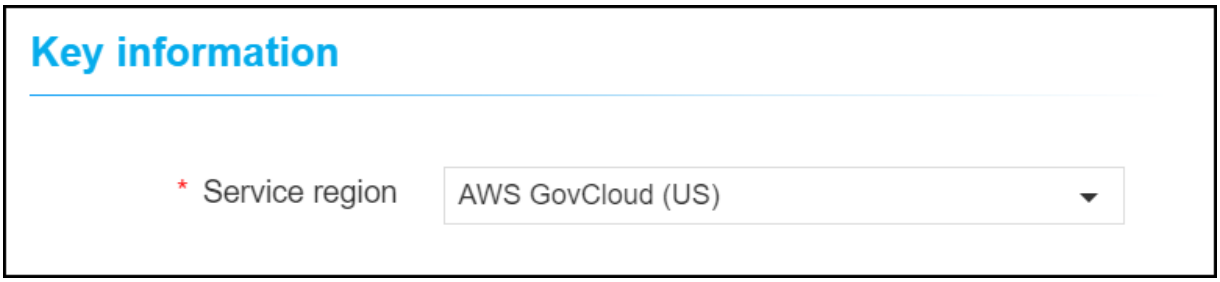


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
Credential type	Dropdown	Yes	**Manual entry**: The user should enter the Access key ID and Secret access key.	NA

Name	Type	Mandatory	Description	Validation
			 **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	
Access key id *	Text	Yes	Access key id of the AmazonELB device.	NA
Secret access key *	Text	Yes	Secret access key of the AmazonELB device.	NA

9. Enter or select the field information in the **Key information** section.



10. The following table provides the field description for adding ADC device details in the Key information section:

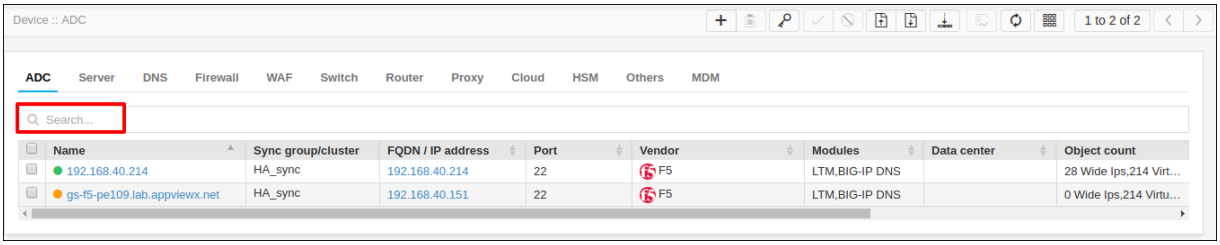
Name	Type	Mandatory	Description	Validation
Service region *	Dropdown	Yes	Service region of the AmazonELB device.	NA

11. Click **Save**.

Validating the Amazon ELB Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



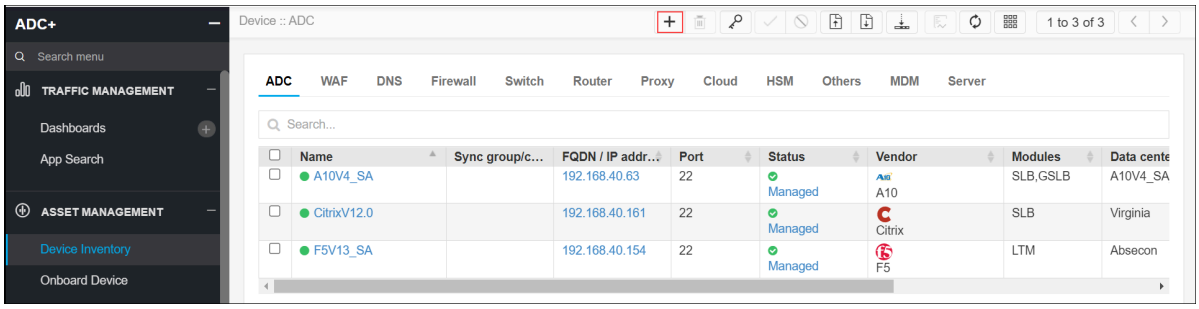
BigIQ

- Adding BigIQ Device
- Validating the BigIQ Device Addition

Adding BigIQ Device

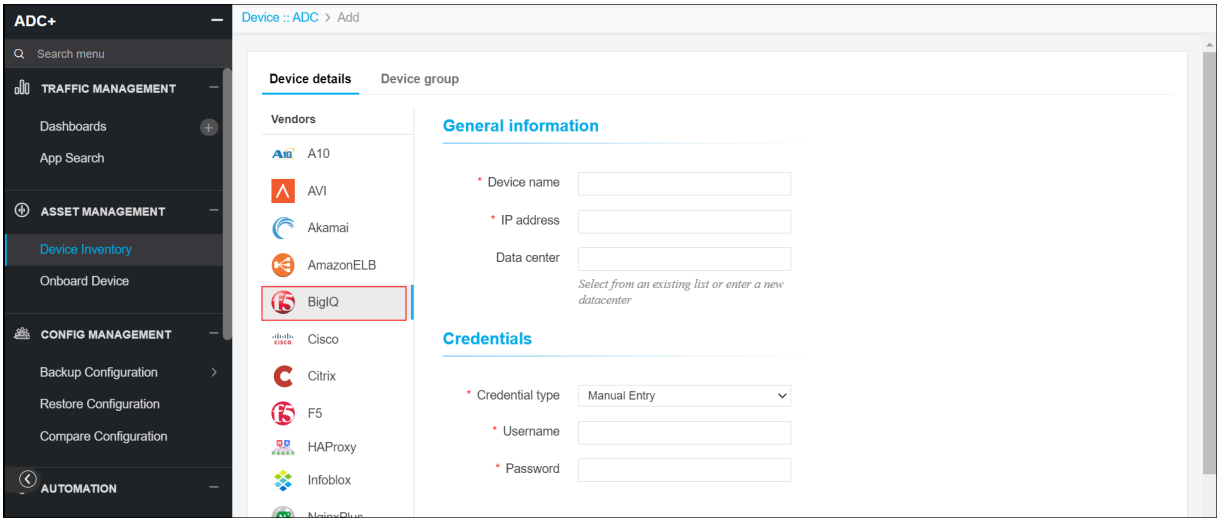
To add BigIQ device,

1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

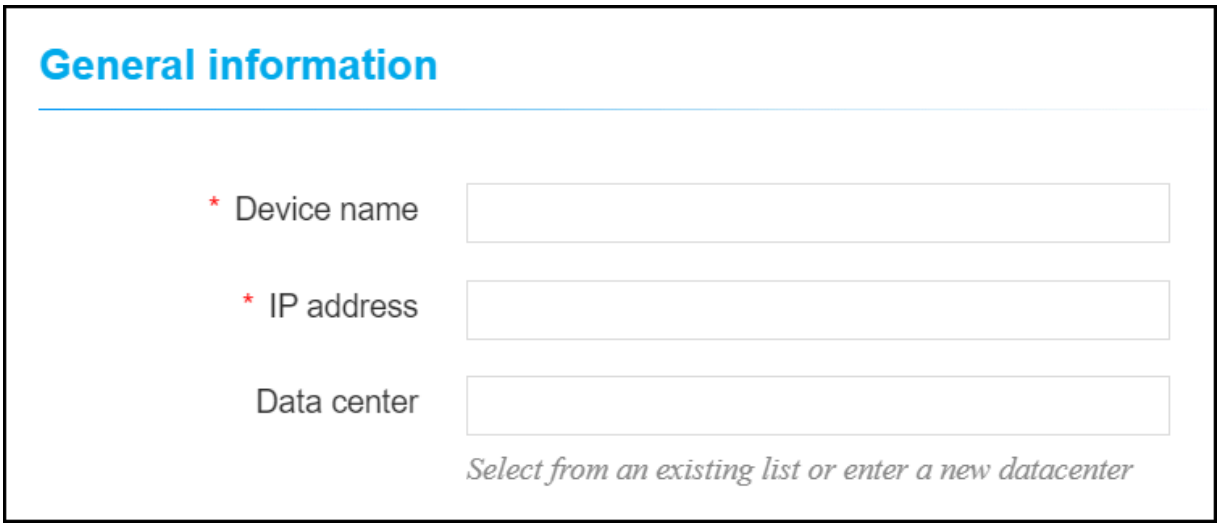


- Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **BigIQ** from the left sidebar.



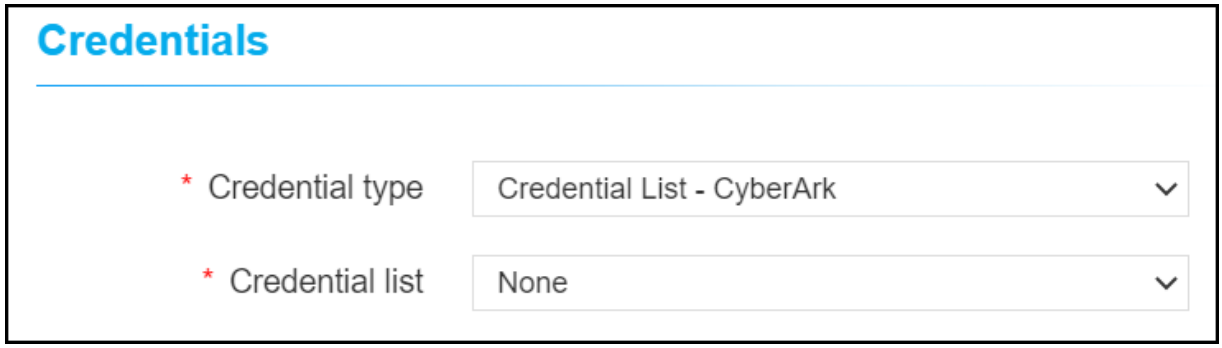
5. Enter or select the field information in the **General information** section.



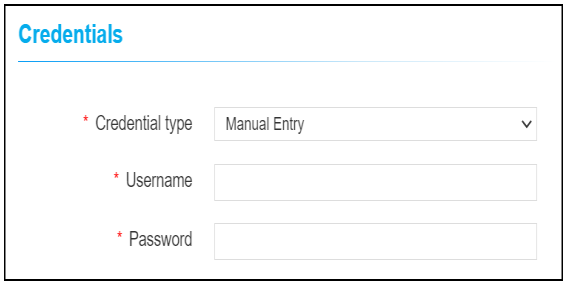
6. The following table provides the field description for adding ADC device details in the **General information** section:

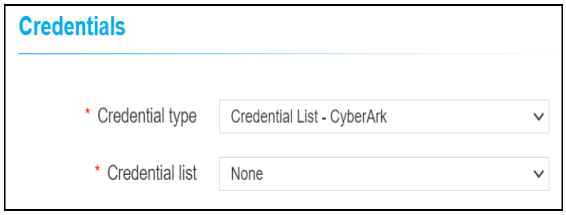
Name	Type	Mandatory	Description	Validation
*Device name	Text	Yes	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
*IP Address	Text	Yes	IP Address of the BigIQ device.	IP address should be in IPv4 format.
Data center	Text	No	Datacenter name where the device is configured. Default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password. 	NA

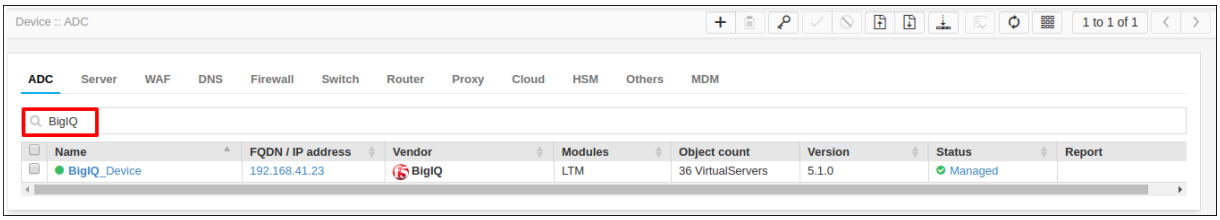
Name	Type	Mandatory	Description	Validation
			Credential List: The user can select the credential details which are already stored in the credential inventory page. 	
*Username	Text	Yes	Username of the BigIQ device.	NA
*Password	Text	Yes	Password of the BigIQ device.	NA

9. Click **Save**.

Validating the BigIQ Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



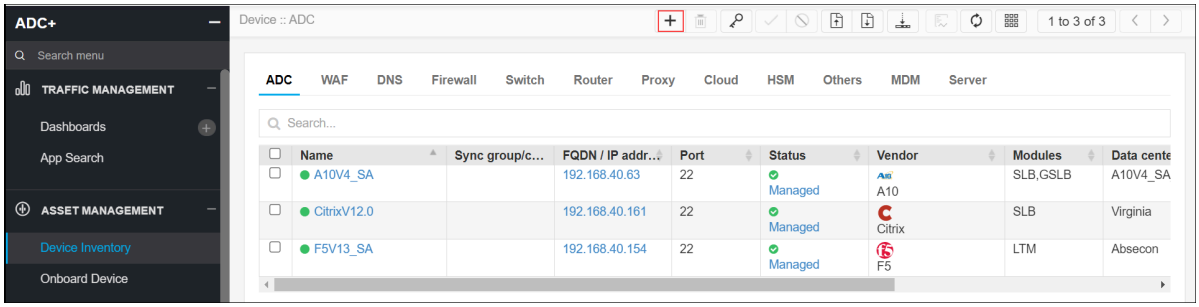
Cisco

- Adding Cisco Device
- Validating the Cisco Device Addition

Adding Cisco Device

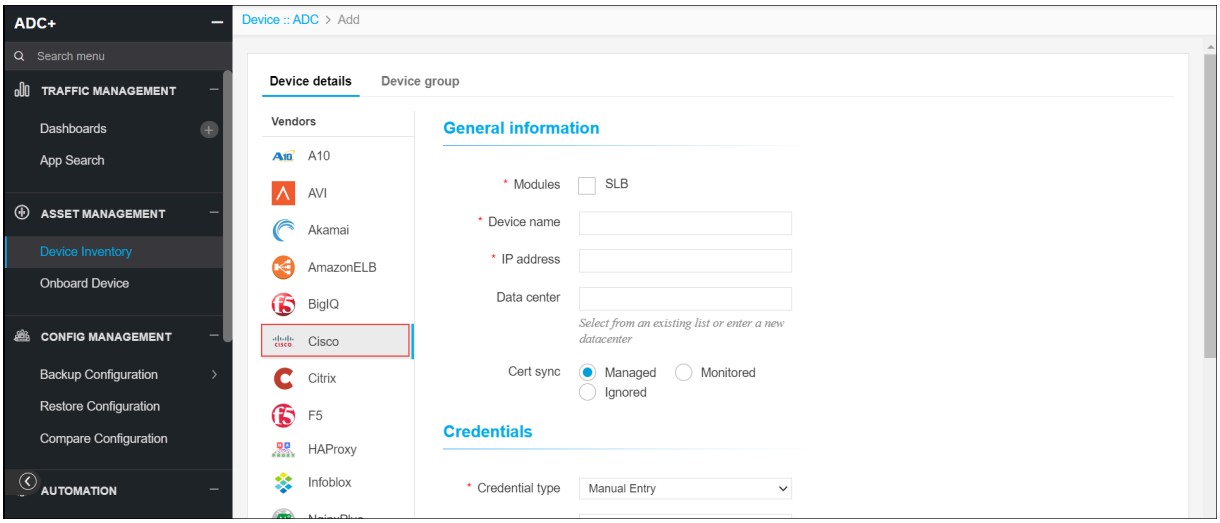
To add Cisco device,

1. Log in to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

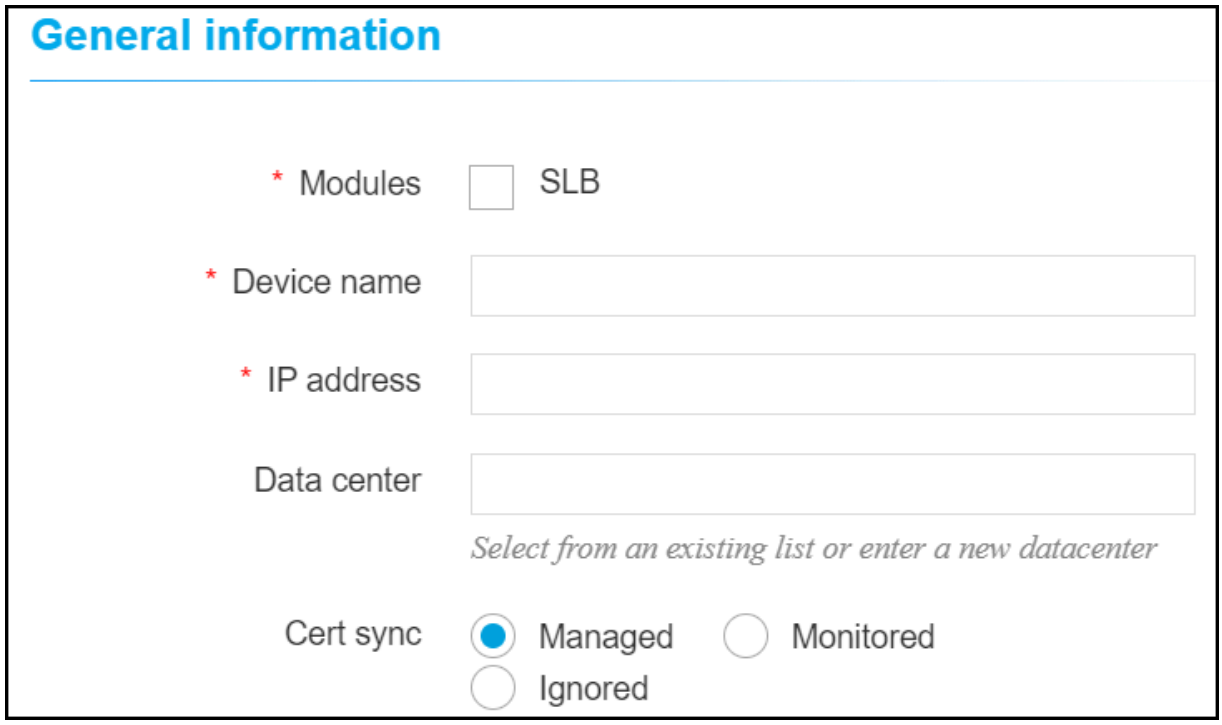


   - Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **Cisco** from the left sidebar.



5. Enter or select the field information in the **General information** section.

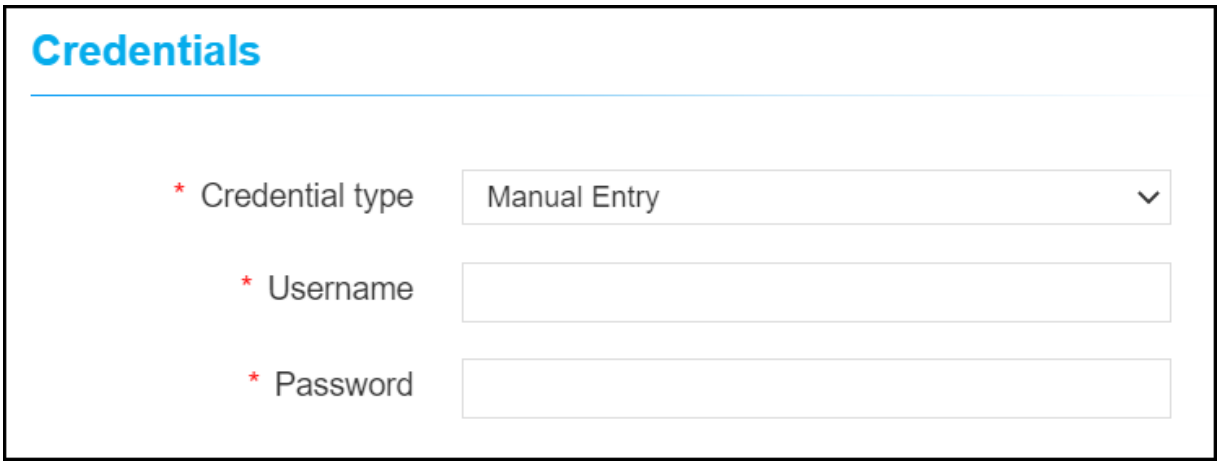


6. The following table provides the field description for adding ADC device details in the **General information** section:

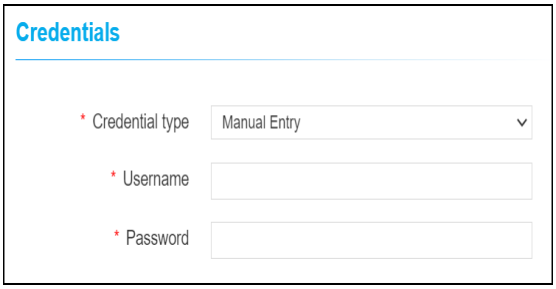
Name	Type	Mandatory	Description	Validation
*Module	Check box	Yes	SLB Module.	NA
*Device name	Text	Yes	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
*IP Address	Text	Yes	IP Address of the BigIQ device.	IP address should be in IPv4 format.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
*Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**:	NA

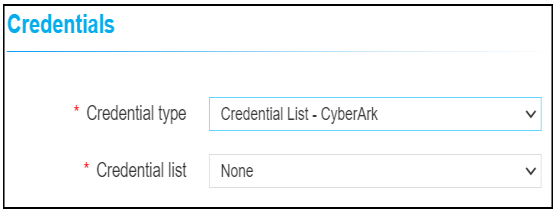
Name	Type	Mandatory	Description	Validation
			The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

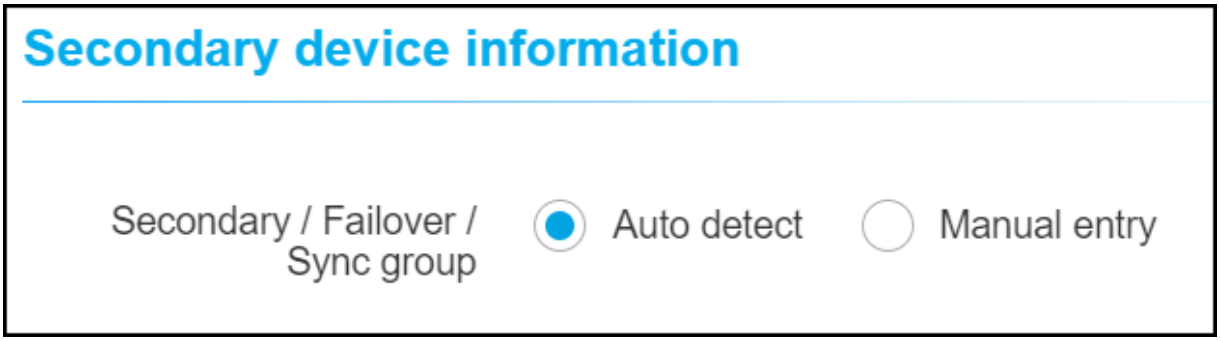


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password. 	NA

Name	Type	Mandatory	Description	Validation
			Credential List: The user can select the credential details which are already stored in the credential inventory page. 	
*Username	Text	Yes	Username of the Cisco device.	NA
*Password	Text	Yes	The password of the Cisco device.	NA

9. Enter or select the field information in the **Secondary device information** section.



10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

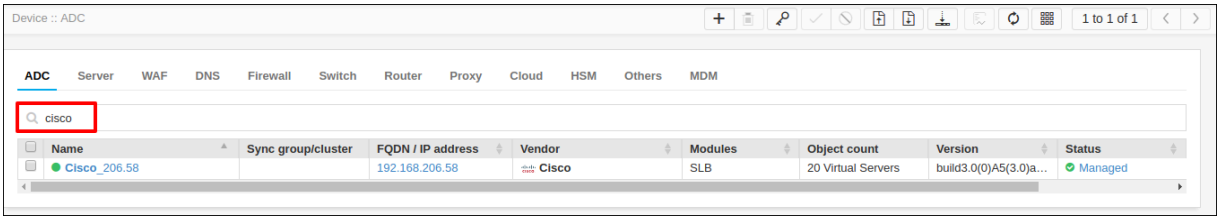
Name	Type	Mandatory	Description	Validation
*Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory. **Manual entry**: The user can use this option to add the peer devices manually.	NA

11. Click **Save**.

Validating the Cisco Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



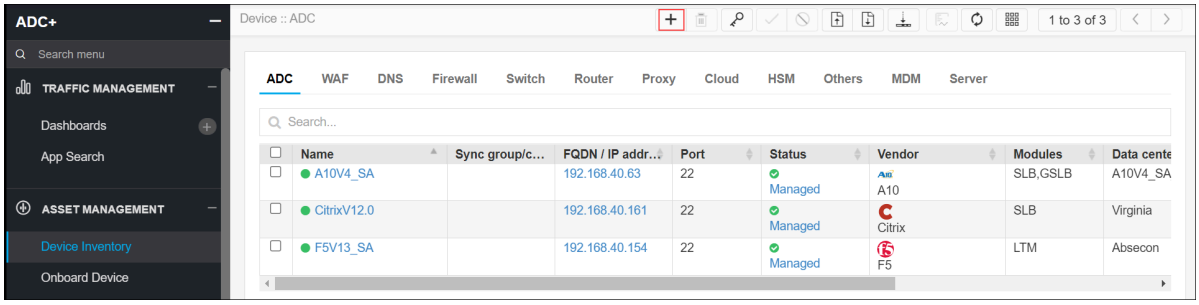
Citrix

- Adding Citrix Device
- Validating the Citrix Device Addition

Adding Citrix Device

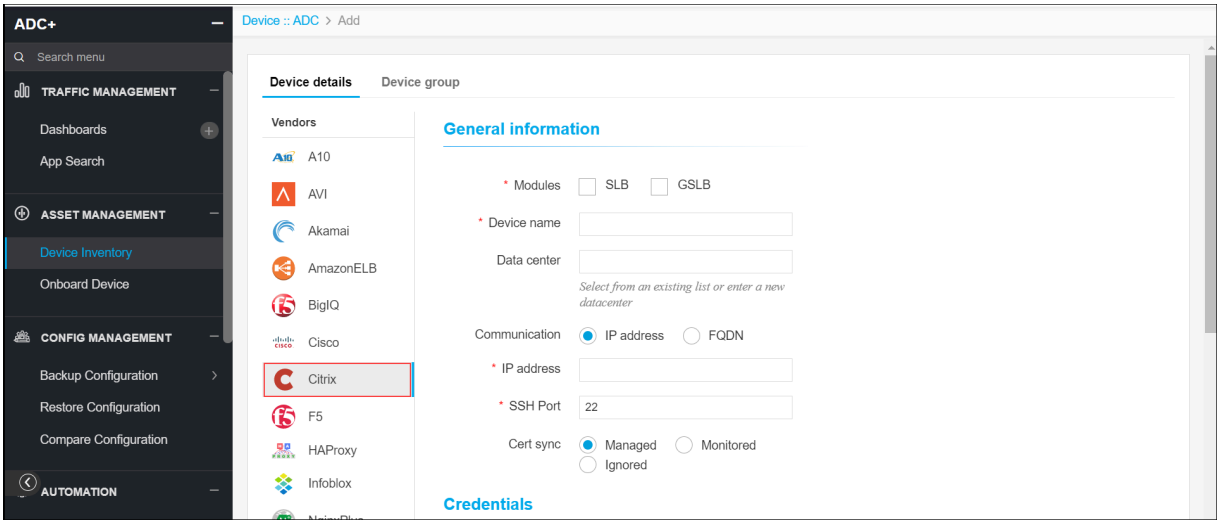
To add Citrix device,

1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

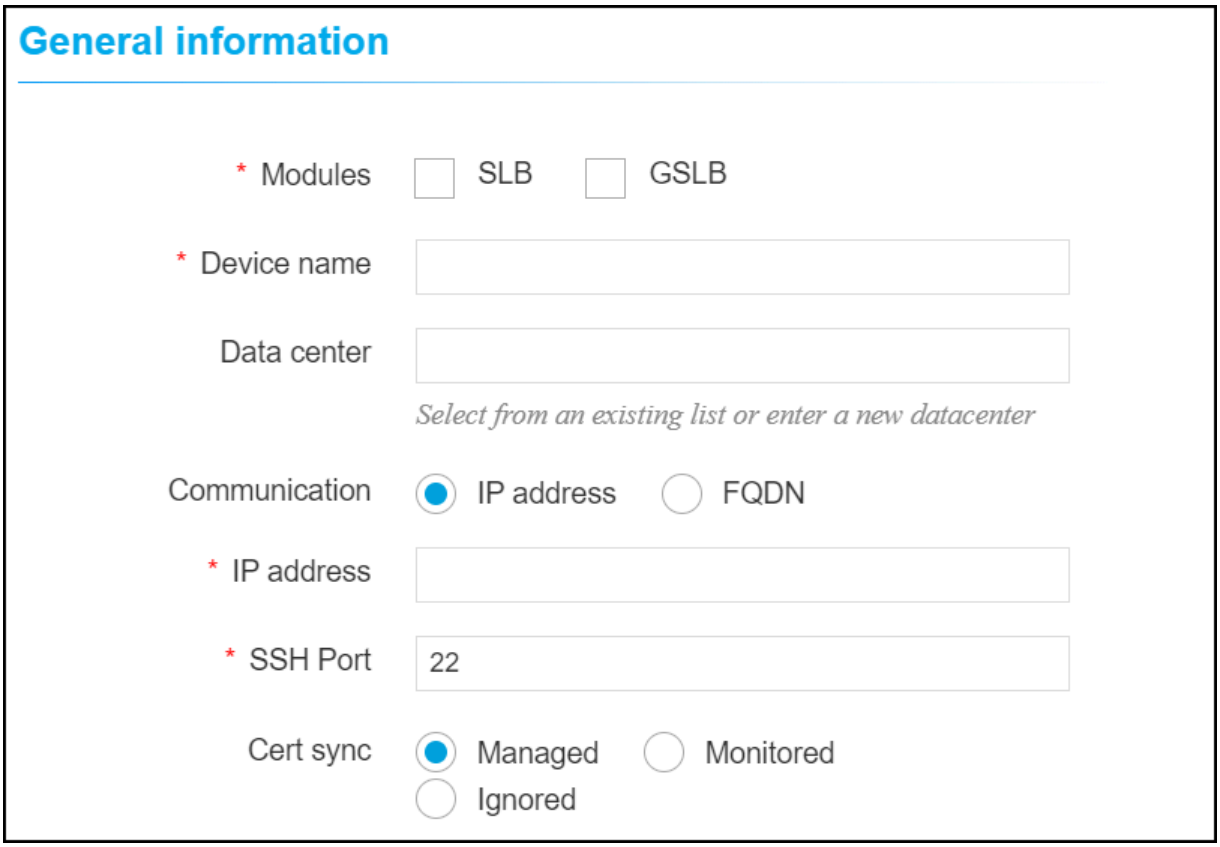


   - Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **Citrix** from the left sidebar.



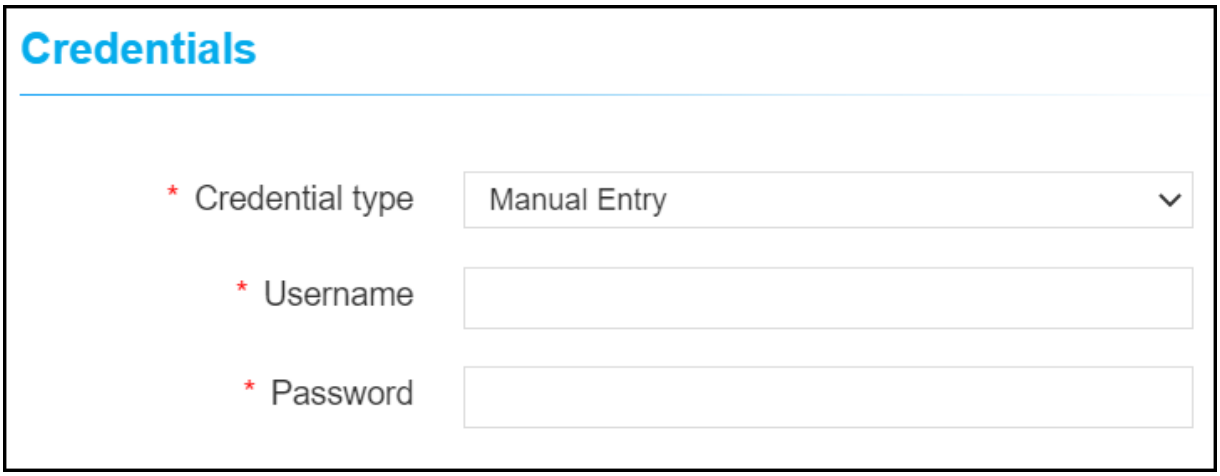
5. Enter or select the field information in the **General information** section.



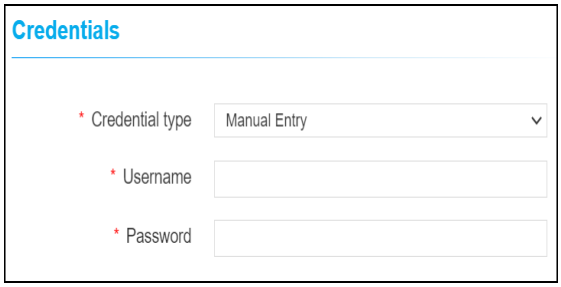
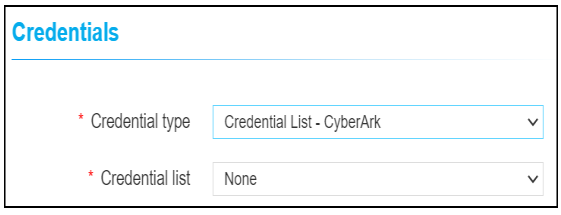
6. The following table provides the field description for adding ADC device details in the **General information** section:

Name	Type	Mandatory	Description	Validation
*Module	Check box	Yes	SLB / GSLB Module.	NA
*Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
*Communication	Radio button	Yes	Devices can be accessed using an IP address or FQDN.	NA
*IP Address	Text	Yes	The ipv4 address of the device.	The IP address should be in the right format.
*FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.
*SSH Port	Text	Yes	Communication port of the device.	Numbers only.
*Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	NA

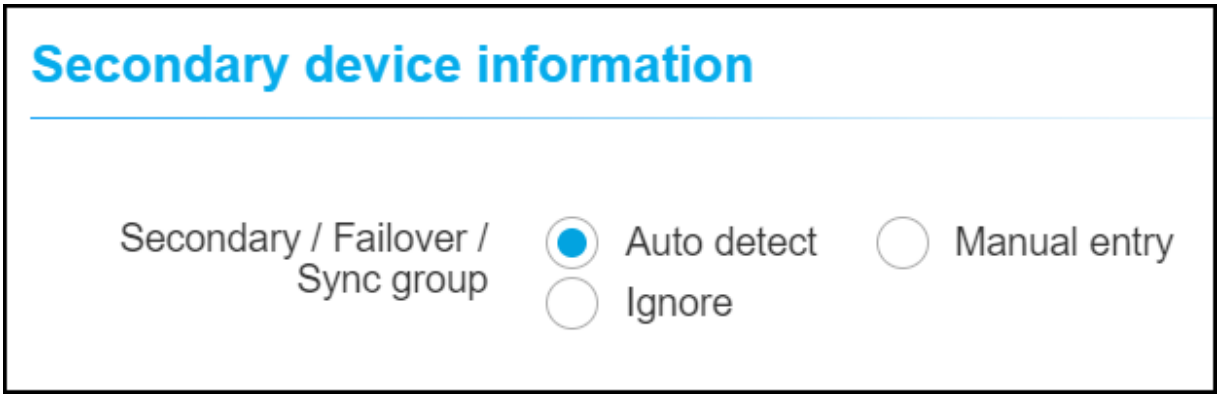
7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	NA
*Username	Text	Yes	The user name of the device.	NA
*Password	Text	Yes	The password of the device.	NA

9. Enter or select the field information in the **Secondary device information** section.



10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

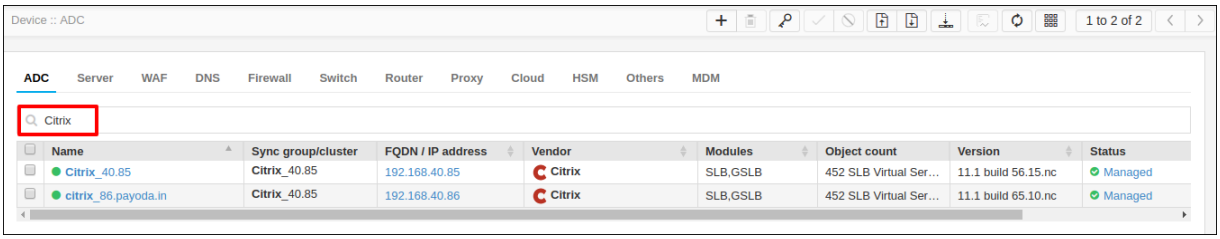
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

11. Click **Save**.

Validating the Citrix Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select ☰ **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.

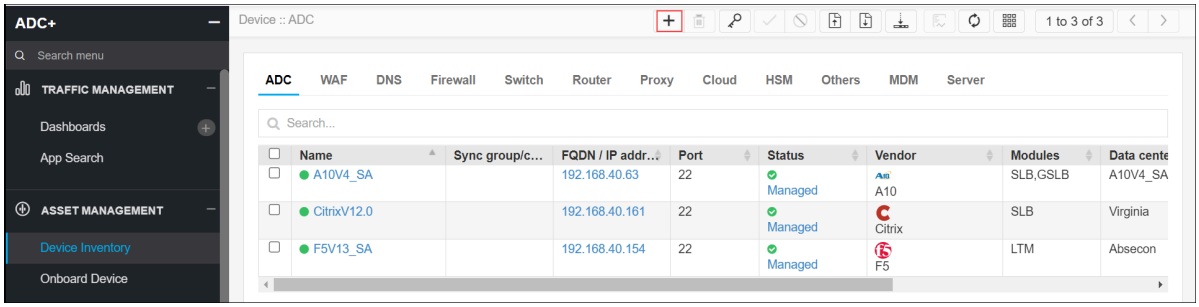


F5

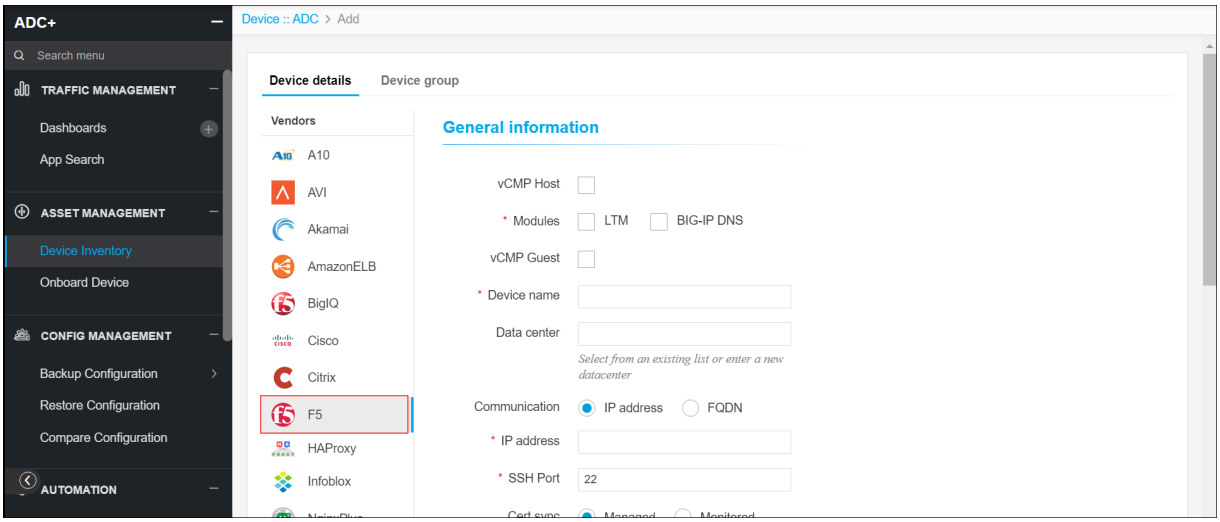
Adding F5 Device

To add F5 device,

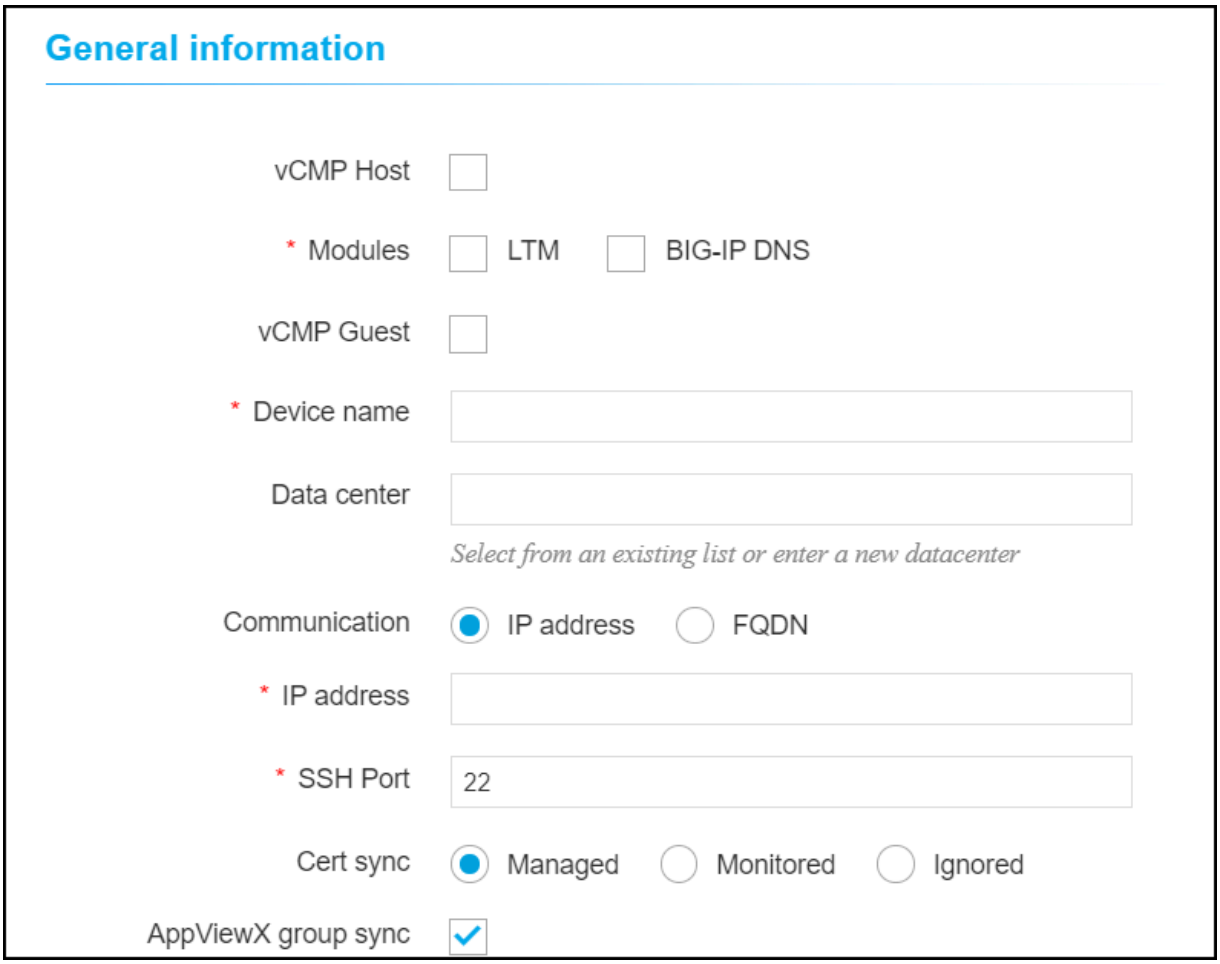
1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - Click **Onboard Device** in the left navigation panel.
4. In the **Device details** page, click on the **F5** icon.



5. Enter or select the field information in the **General information** section.

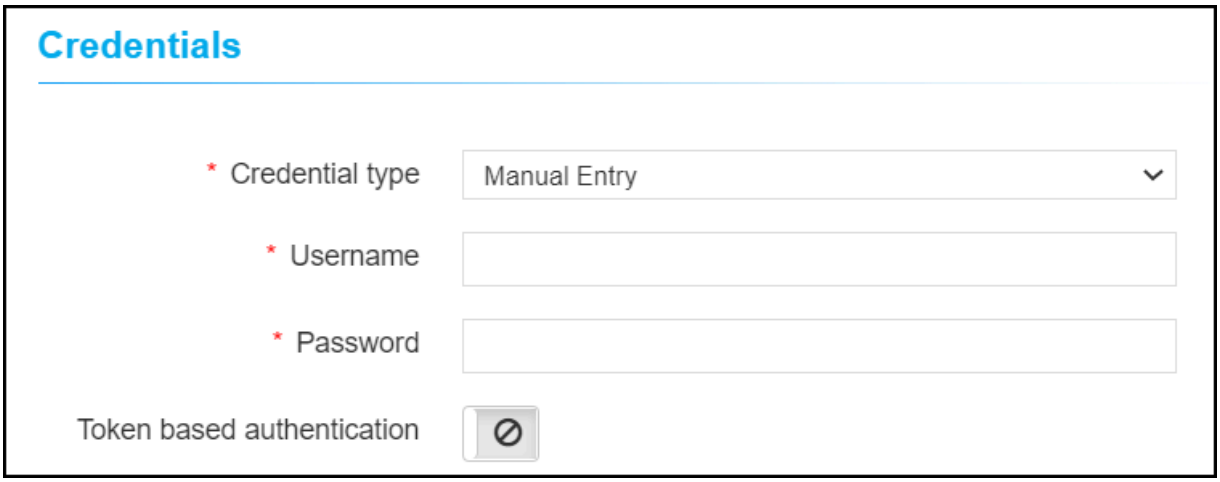


6. The following table provides the field description for adding ADC device details in the **General information** section:

Name	Type	Mandatory	Description	Validation
VCMP Host	Check box	No	To add a device as a vcmb host, this checkbox should be checked.	NA
*Module	Check box	Yes	LTM / BIG-IP DNS Module.	NA
VCMP Guest	Check box	No	To add a device as a vcmp guest, this checkbox should be checked.	NA
*Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Data center name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
*Communication	Radio button	Yes	Devices can be accessed using an IP address or FQDN.	NA
*IP Address	Text	Yes	The ipv4 address of the device.	The IP address should be a valid IPv4 format.
*FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.
*SSH Port	Text	Yes	Communication port of the device.	Numbers only.
*Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**:	NA

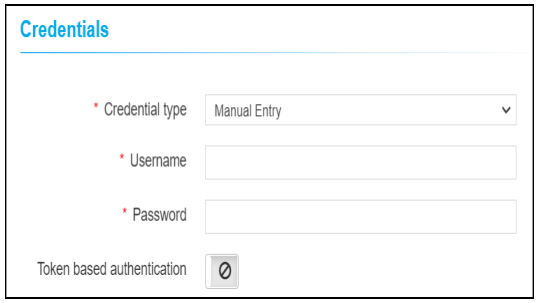
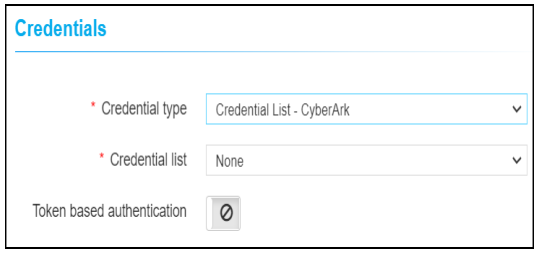
Name	Type	Mandatory	Description	Validation
			The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	
AppViewX Group Sync	Check box	No	This should be enabled if the user wants to sync the devices within the device group.	NA

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

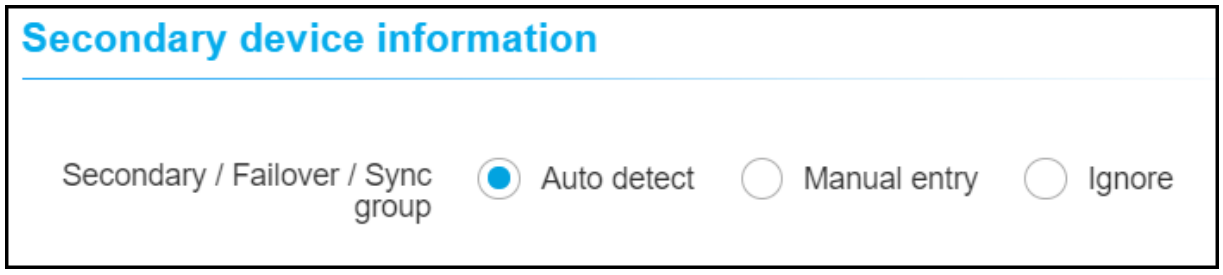


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.	NA

Name	Type	Mandatory	Description	Validation
			 **Credential List**: The user can select the credential details which are already stored in the credential inventory page. For more details on secure authentication, refer to Platform User Guide. 	
*Username	Text	Yes	The user name of the device.	NA
*Password	Text	Yes	The password of the device.	NA
Token based authentication	Toggle button	No	To access the device REST API using token.	NA

9. Enter or select the field information in the **Secondary device information** section.



10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

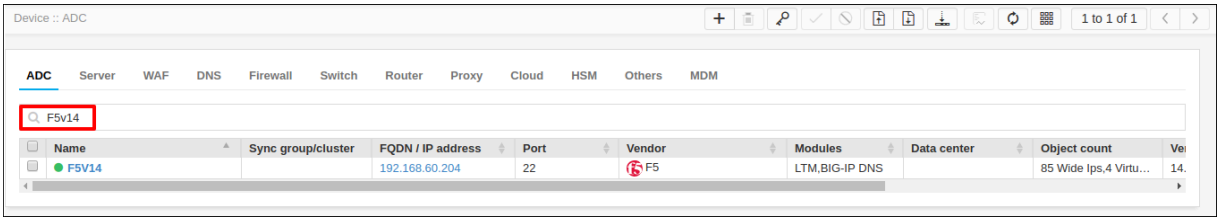
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

11. Click **Save**.

Validating F5 Device Addition

After adding the device, you can validate the device by searching the device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. From the device inventory page, search for the added F5 device name.



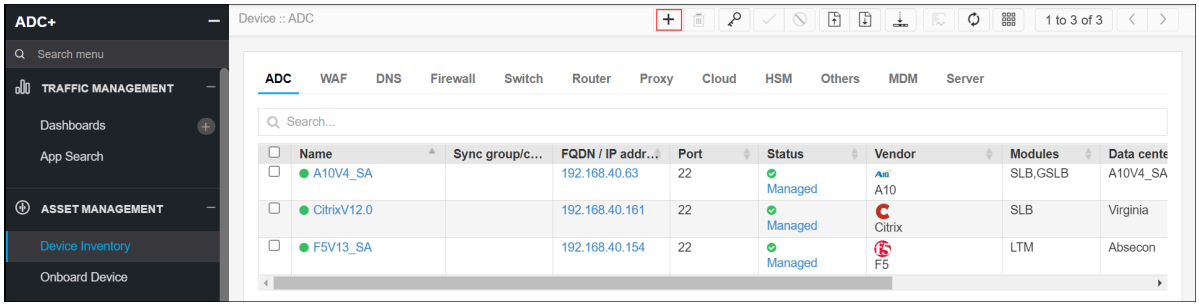
HAProxy

- Adding HAProxy Device
- Validating the HAProxy Device Addition

Adding HAProxy Device

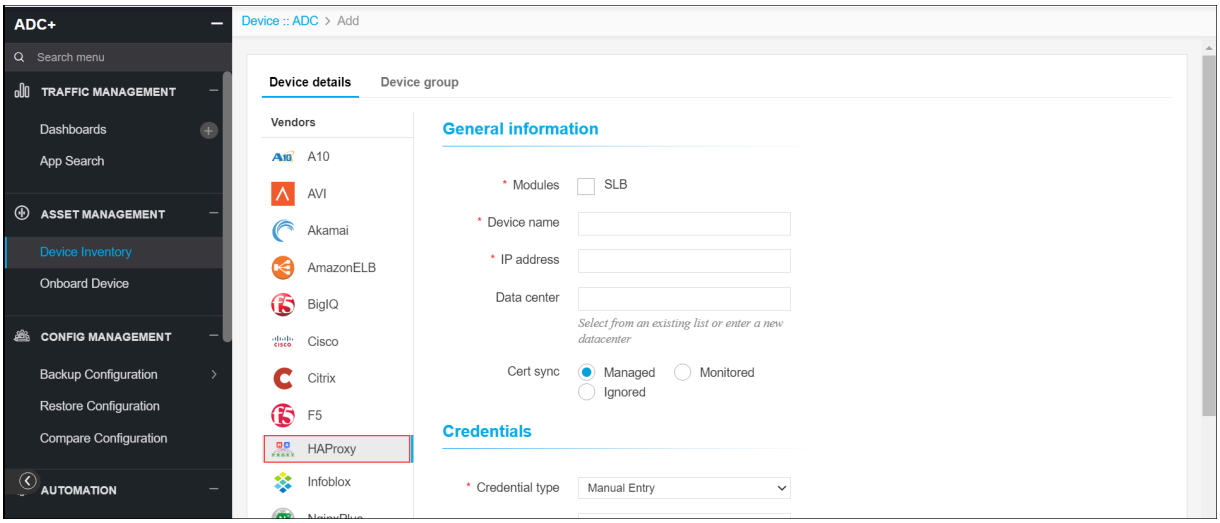
To add HAProxy device,

1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

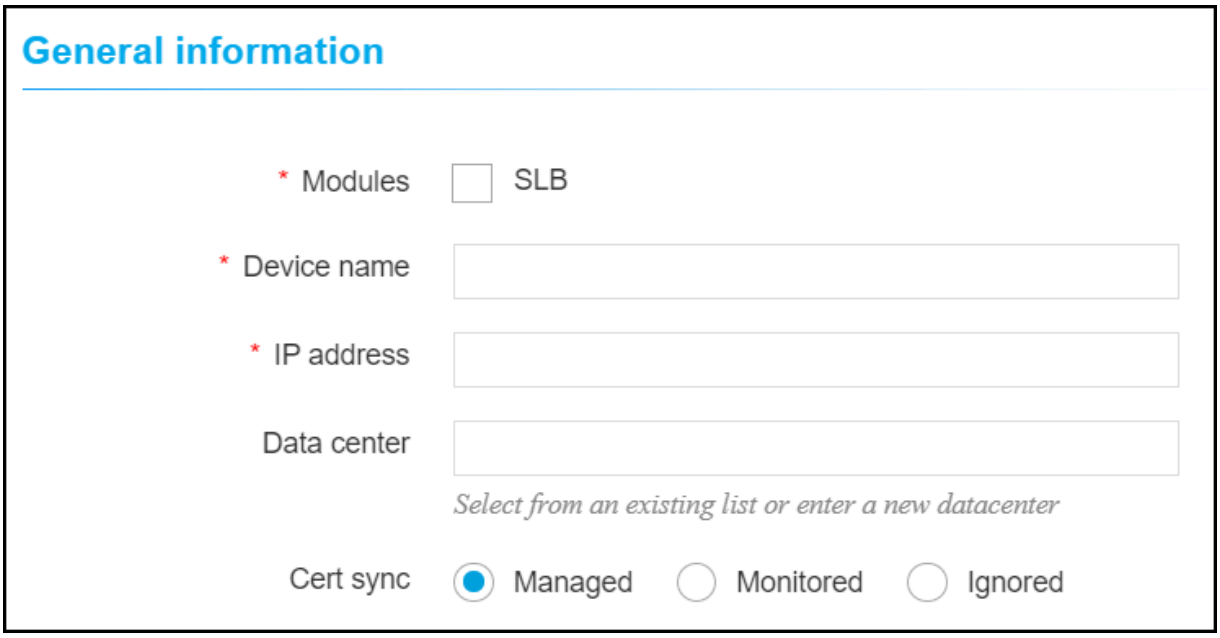


   - Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **HAProxy** from the left sidebar.



5. Enter or select the field information in the **General information** section.

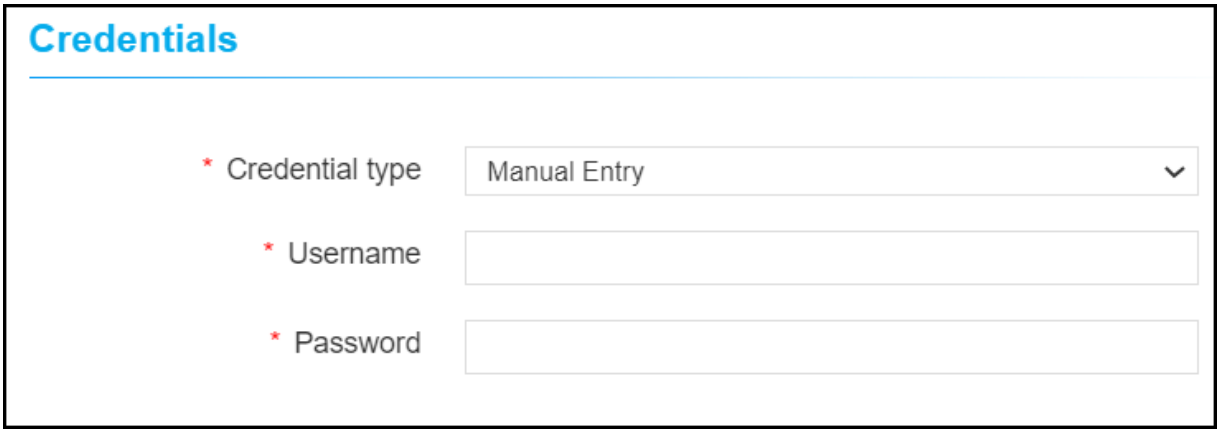


6. The following table provides the field description for adding ADC device details in the **General information** section:

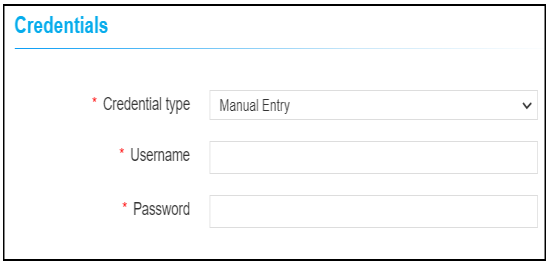
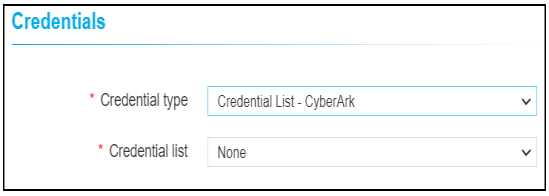
Name	Type	Mandatory	Description	Validation
Device name *	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
IP Address *	Text	Yes	The ipv4 address of the device.	The IP address should be in the right format.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Cert Sync *	Radio button	Yes	Managed: The certificates of the device can be managed. Monitored: The certificates of the device can be monitored. Ignored:	NA

Name	Type	Mandatory	Description	Validation
			The certificate sync can be ignored.	

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	NA

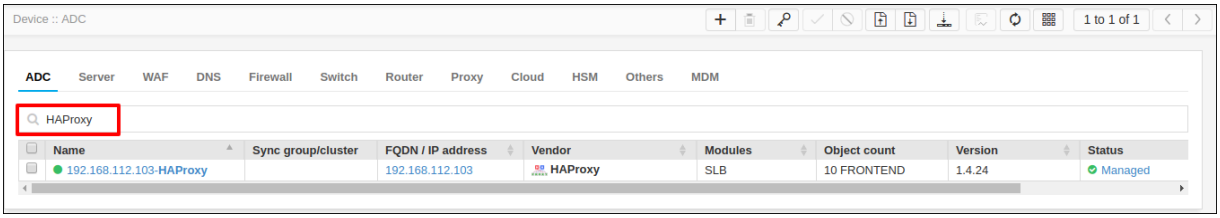
Name	Type	Mandatory	Description	Validation
*Username	Text	Yes	The user name of the device.	NA
*Password	Text	Yes	The password of the device.	NA

9. Click **Save**.

Validating the HAProxy Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



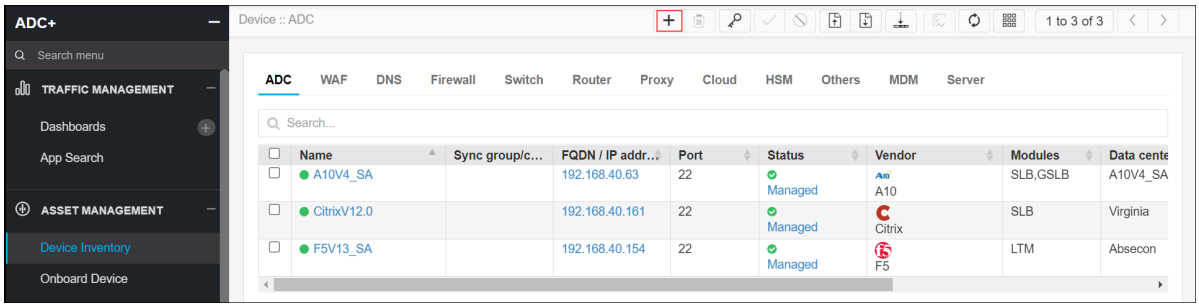
InfoBlox

- Adding InfoBlox Device
- Validating the Infoblox Device Addition

Adding InfoBlox Device

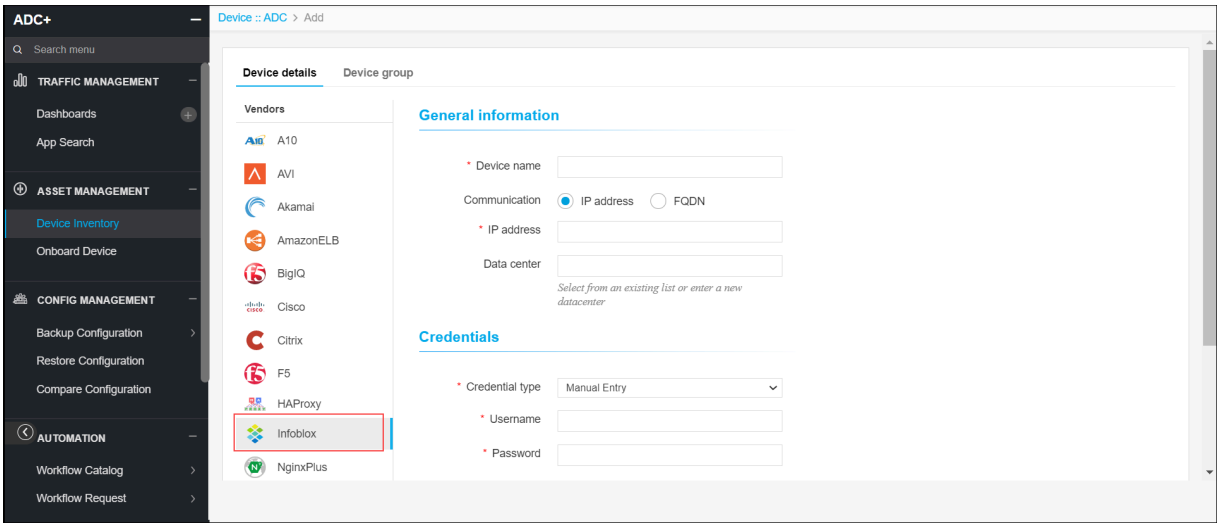
To add InfoBlox device,

1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.

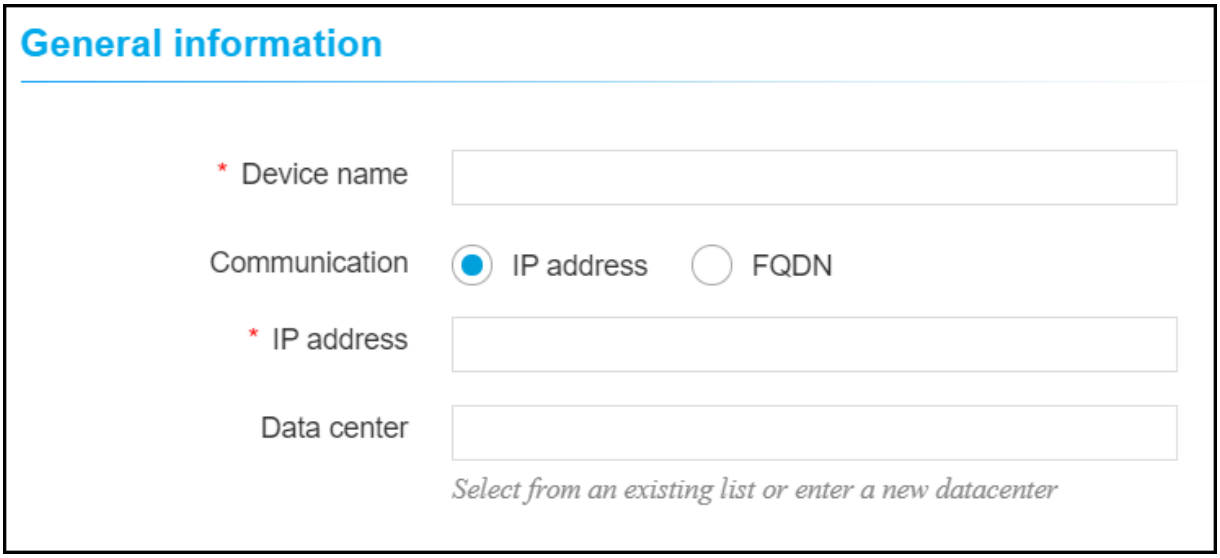


- Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, select **Infoblox** from the left sidebar.



5. Enter or select the field information in the **General information** section.



6. The following table provides the field description for adding ADC device details in the **General information** section:

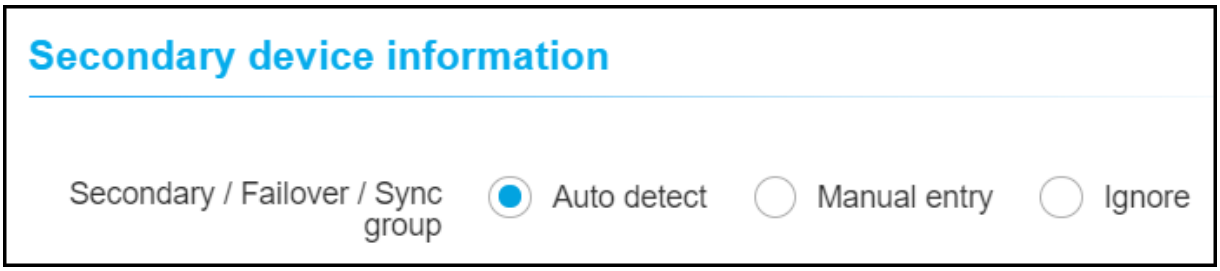
Name	Type	Mandatory	Description	Validation
*Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
*Communication	Radio button	Yes	Devices can be accessed using an IP address or FQDN.	NA
*IP Address	Text	Yes	The ipv4 address of the device.	The IP address should be in the right format.
*FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.

7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.

8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password. **Credential List**: The user can select the credential details which are already stored in the credential inventory page.	NA
*Username	Text	Yes	The user name of the device.	NA
*Password	Text	Yes	The password of the device.	NA

9. Enter or select the field information in the **Secondary device information** section.



10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

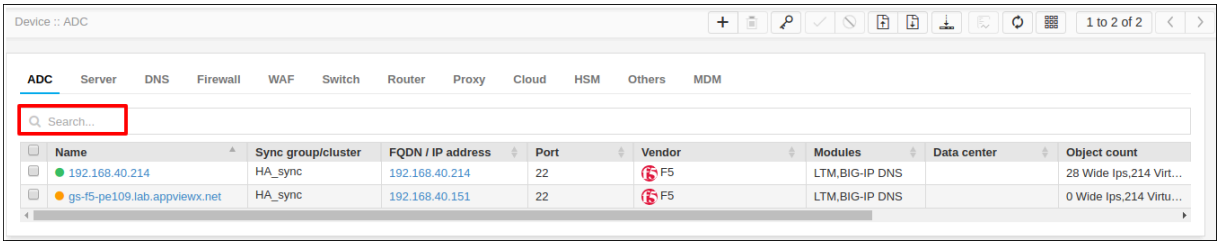
Name	Type	Mandatory	Description	Validation
Secondary / Failover / Sync group	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The user can use this option to ignore the auto-detection of the peer devices.	NA

11. Click **Save**.

Validating the Infoblox Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.



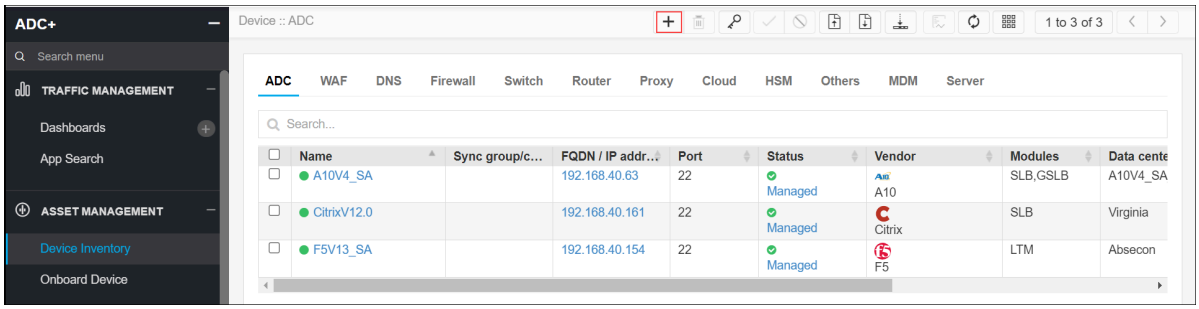
NginxPlus

- Adding NginxPlus Device
- Validating the NginxPlus Device Addition

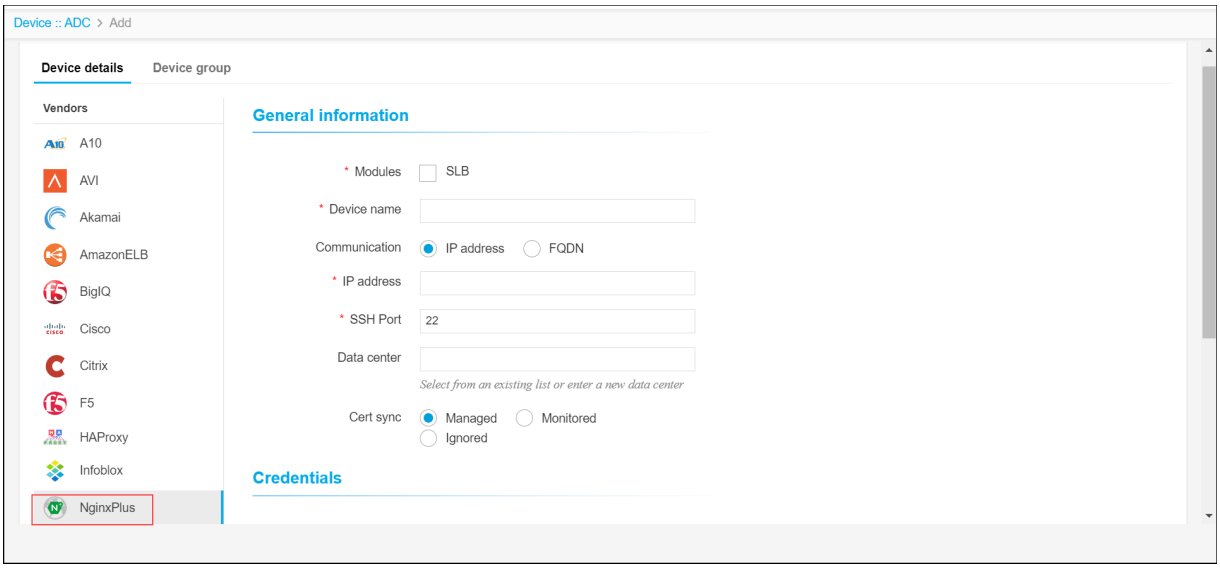
Adding NginxPlus Device

To add NginxPlus device,

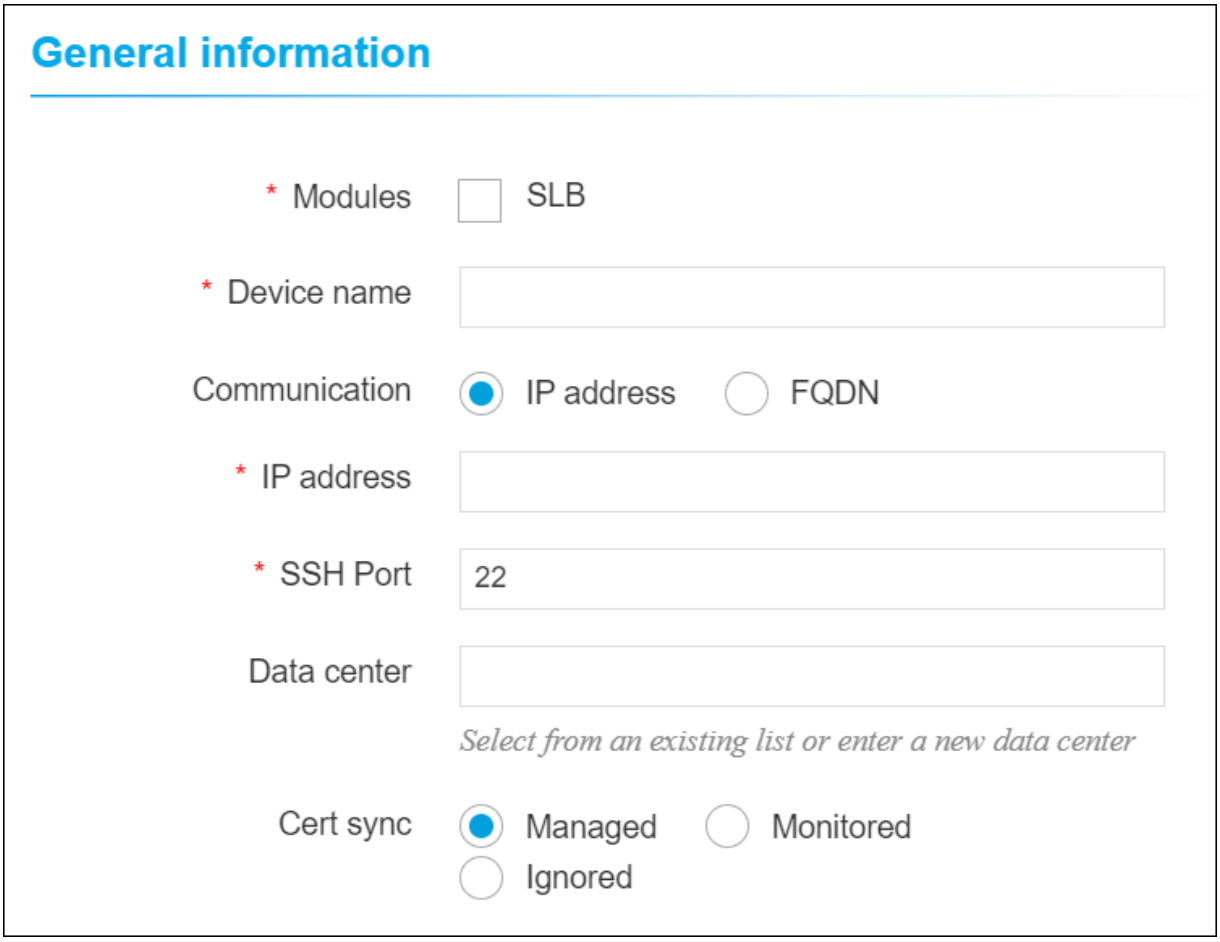
1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - Click **Onboard Device** in the left navigation panel.
4. In the **Device details** page, select **NginxPlus** from the left sidebar.



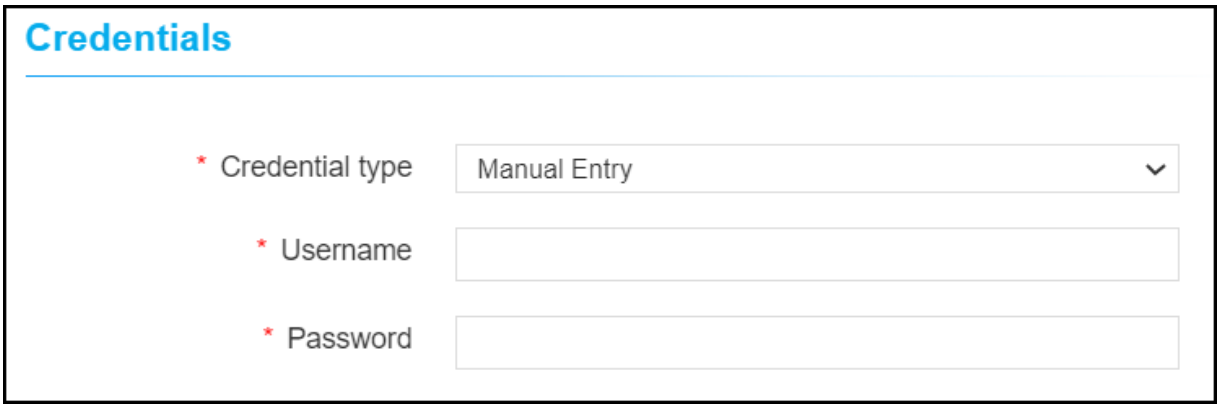
5. Enter or select the field information in the **General information** section.



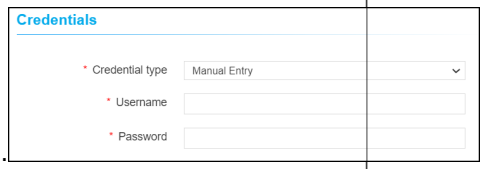
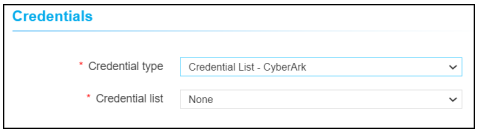
6. The following table provides the field description for adding ADC device details in the **General information** section:

Name	Type	Mandatory	Description	Validation
Modules	Check box	Yes	SLB	NA
Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Communication	Radio button	No	Devices can be accessed using an IP address or FQDN.	No
IP Address	Text	Yes	The IPv4 address of the device.	The IP address should be in the right format.
SSH Port	Text	Yes	Communication port of the device.	Numbers only.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.
Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be monitored. **Ignored**: The certificate sync can be ignored.	NA

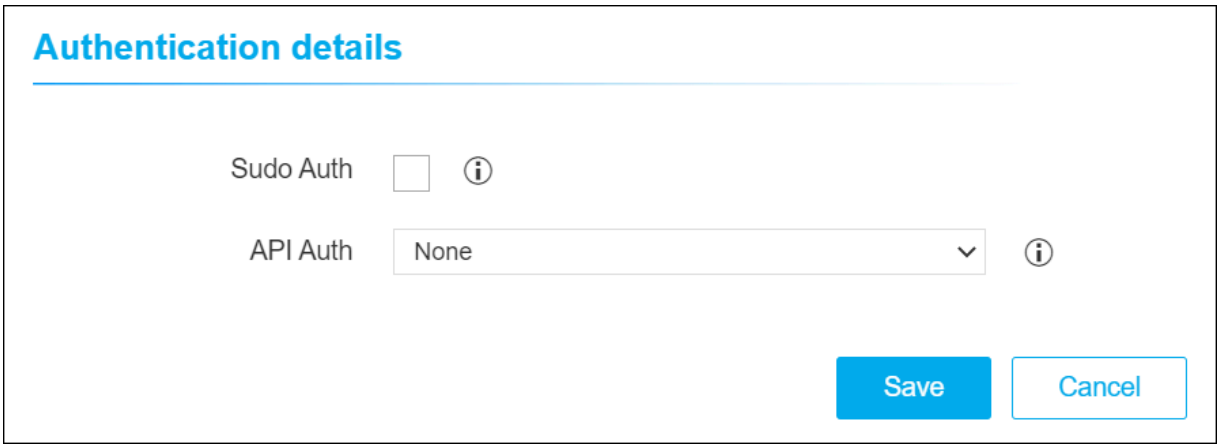
7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
Credential type	Dropdown	Yes	Manual entry: The user should enter the username and password.  Credential List: The user can select the credential details which are already stored in the credential inventory page. 	NA
Username	Text	Yes	The user name of the device.	NA
Password	Text	Yes	The password of the device.	NA

9. Enter or select the field information in the **Authenticaion details** section.



10. The following table provides the field description for adding ADC device details in the **Authenticaion details** section:

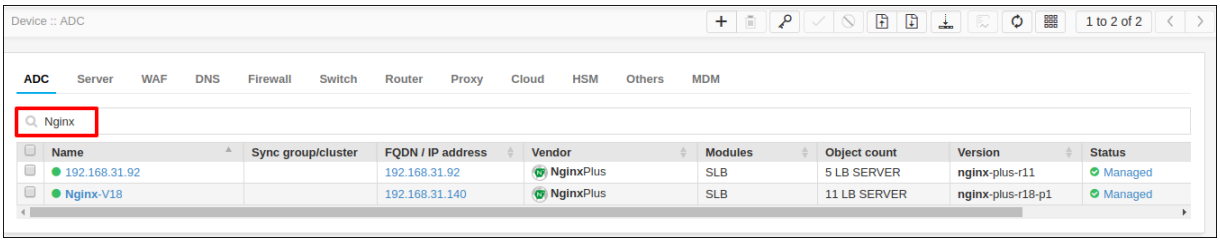
Name	Type	Mandatory	Description	Validation
Sudo Auth	Checkbox	No	select the **Sudo Auth** checkbox in the to enable the Sudo authentication for a non-root user credentials.	
API Auth	Dropdown	No	This option allows the basic or token based authentication for API enabled devices. The options are: • **Basic Auth** - select this option to configure HTTP authentication with password. You can choose device credentials or manual entry. • **Token Auth** - select this option to enter the JSON Web tokens for token based authentication.	

11. Click **Save**.

Validating the NginxPlus Device Addition

After adding the device, you can validate the device by searching device in the device inventory.

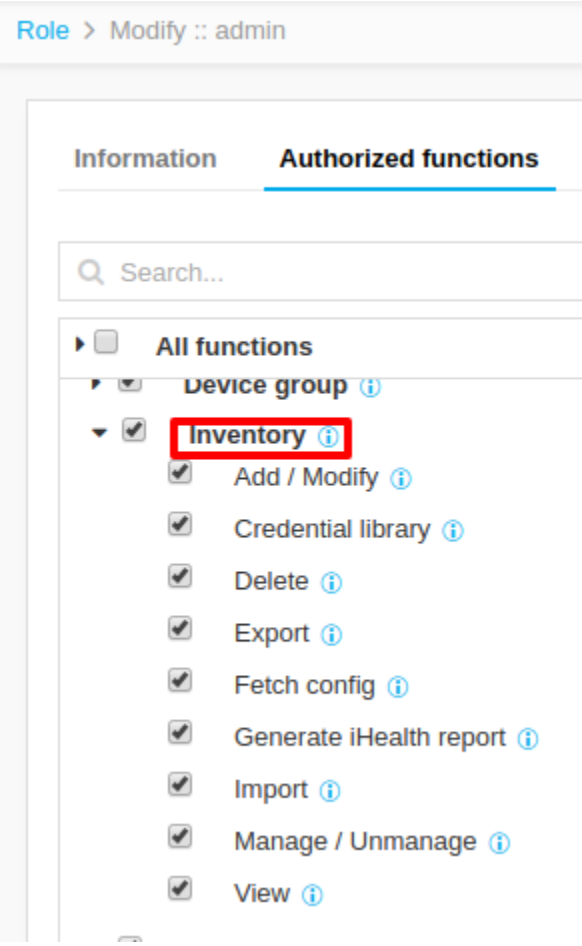
1. Select **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
2. Search the device name and validate whether the device is added successfully.


Device :: ADC
1 to 2 of 2
ADC
Server
WAF
DNS
Firewall
Switch
Router
Proxy
Cloud
HSM
Others
MDM
Nginx
Name
Sync group/cluster
FQDN / IP address
Vendor
Modules
Object count
Version
Status
192.168.31.92
192.168.31.92
NginxPlus
SLB
5 LB SERVER
nginx-plus-r11
Managed
Nginx-V18
192.168.31.140
NginxPlus
SLB
11 LB SERVER
nginx-plus-r18-p1
Managed

Chapter 3: Inventory Actions

Before You Begin

To do any actions in the ADC-inventory, the user should have ACF permissions to access the inventory page and its various actions as mentioned in the screenshot.



Deleting ADC Device(s)

To delete ADC device(s),

1. Go to ☰ **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Select the desired ADC device(s) to delete.
3. Click the 🗑 **Delete** button in the Command bar.
   The **Delete** confirmation modal appears.

4. Click **Yes** to delete the selected ADC device(s).

> **Note:** To discard the deletion, click **No**. Note: The device details and configurations will be permanently deleted from AppViewX. Note: If the deleted device is onboarded again, it will be considered as onboarding a new device.

Import Devices

Device import provides a hassle-free experience in onboarding multiple ADC devices into AppViewX in one single step. For onboarding multiple devices, the details should be filled in the excel sheet in the predefined format and can be uploaded to AppViewX and from there AppViewX will dynamically onboard all the devices available in the sheet.

To import devices using a `.csv` file,

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Click the **Import** button in the Command bar.
3. On the Import screen that appears, navigate to the location of the import file, then select it.
4. Click **Import** to add the devices and their details to the Inventory.

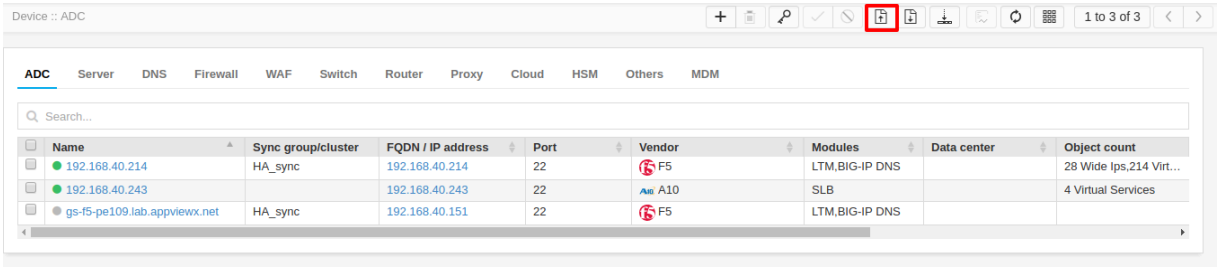
> **Note:** When the file is uploaded with improper structure or incorrect data, the import process will terminate with the errors highlighted.

Export Device Details

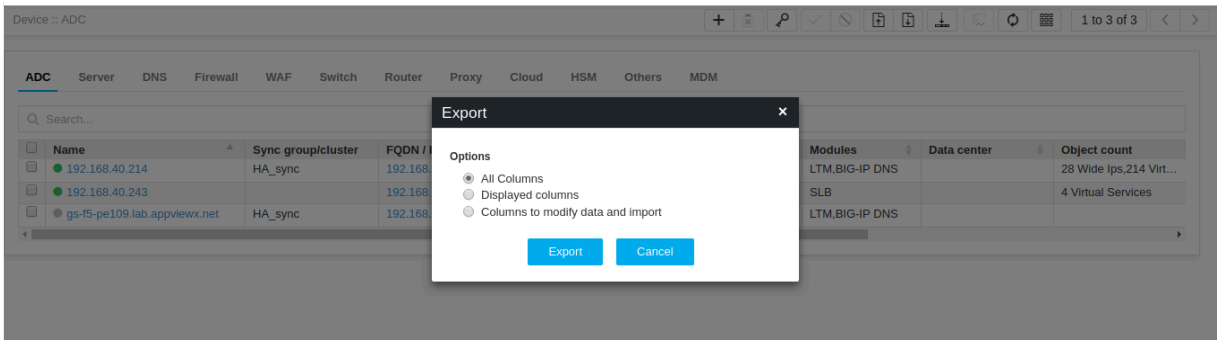
The device details, which are available in the Device Inventory page can be exported into an Excel file.

To export the details of one or more devices,

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. If the device you want to export is not listed on the screen, run a search to locate it.
3. Click the checkbox beside the device name. If you are exporting details of multiple devices of the same kind, select the checkboxes for each one.
4. Click the **Export** button in the Command bar at the upper right of the screen.



5. On the **Export** pop-up screen that appears, select the type of information you want to export:



- **All Columns** - Select this option if you want to export all information about the device.
- **Displayed columns** - Select this option if you want to export only the information that is visible on the Device screen. This is useful if you need to compare values or settings for different devices and do not have any need to see the less important data.
- **Columns to modify data and import** - Select this option if you are exporting device details to make modifications and then re-import the data into the Device Inventory.

6. On the screen that opens, select the location where you want the device details file to go, then click **Save**.
7. The details are then downloaded as an Excel (**.xls**) file.

Manage and Unmanage Devices

To manage or unmanage devices,

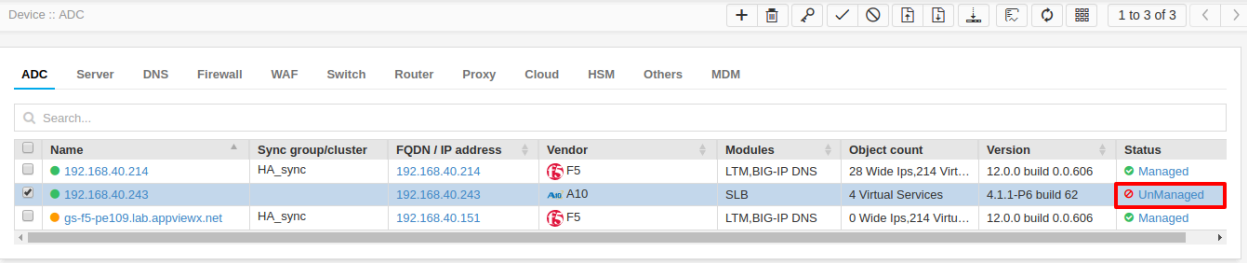
1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. If the device you want to manage or unmanage is not listed on the screen, run a search to locate it.

Note: If you try to manage a device that is already in managed state or unmanage a device that is already in unmanaged state, an error message appears at the top of the screen.

3. Click the checkbox beside the device name.
4. To start managing the device, click the **Manage** button in the Command bar at the top of the screen. To stop managing a device, click the **Unmanage** button.

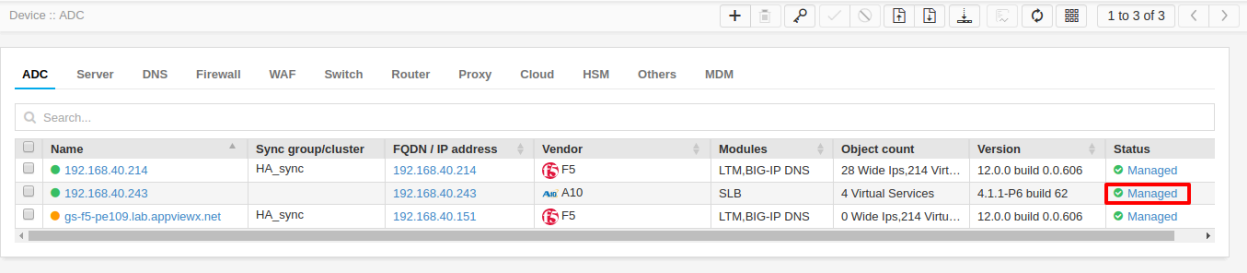
Validating the Unmanage action

The selected devices will be moved to **Unmanaged** status.



Validating the Manage action

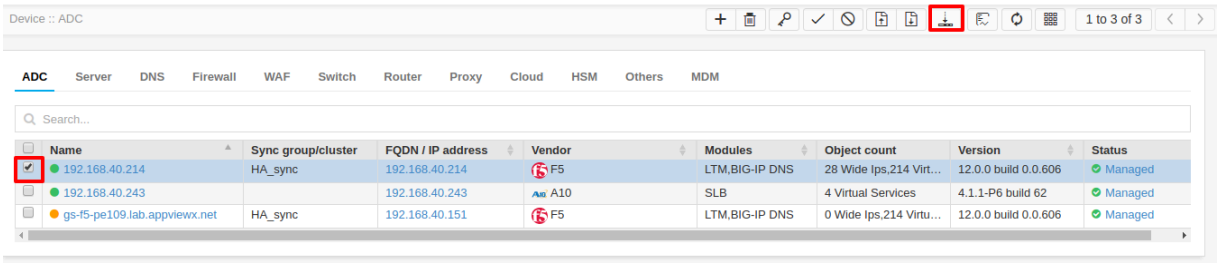
Once the devices are moved from Unmanaged status to Managed status, the config fetch will be triggered to those devices and the device status will be updated.



Config Fetch

This action is being used to fetch and update the device configuration in AppViewX.

1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Device**.
3. Select the devices from the **Device Inventory** page.



4. Click the **Config fetch** icon.

• Validating the Config fetch action

Validating the Config fetch action

Once the config fetch is triggered, the device will be moved to **Queued** status and then **InProgress** status. Eventually, the device status will be updated to **Managed** once the device configuration is downloaded and parsed successfully in the AppViewX.

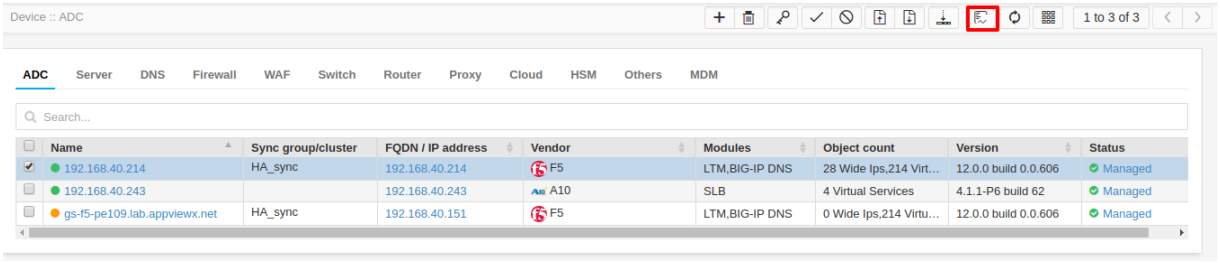
Generate and Download an iHealth Report

BIG -IP iHealth is a diagnostic tool developed by F5 to manage local traffic manager (LTM) and global traffic manager (GTM) devices. The iHealth report provides tailored diagnostic information that gives you valuable, actionable insight into the efficiency of the hardware and software running in your BIG-IP system.

- iHealth reports can be generated at the time you want to view or schedule it in advance through the Workflow.
- To generate an iHealth report, ensure that the proxy is configured in the Settings module. For detailed information, refer to the Proxy Settings section of Platform User guide.

To generate and download an iHealth report,

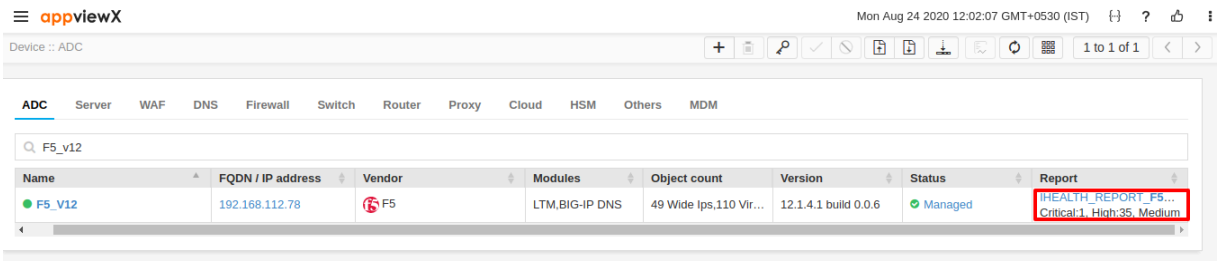
1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**
   By default, the **ADC** tab opens.
2. Select the checkbox beside the ADC device for which you want to generate an iHealth report.



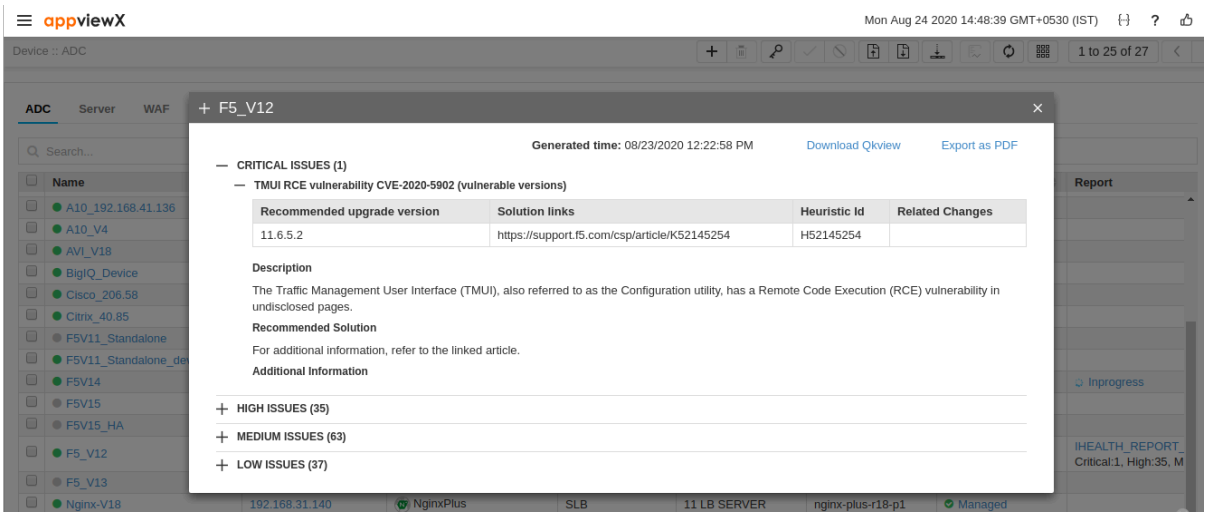
3. Click the **Generate iHealth Report** button ( ) in the Command bar.

> **Note:** You might need to scroll to the right to see the Report column.

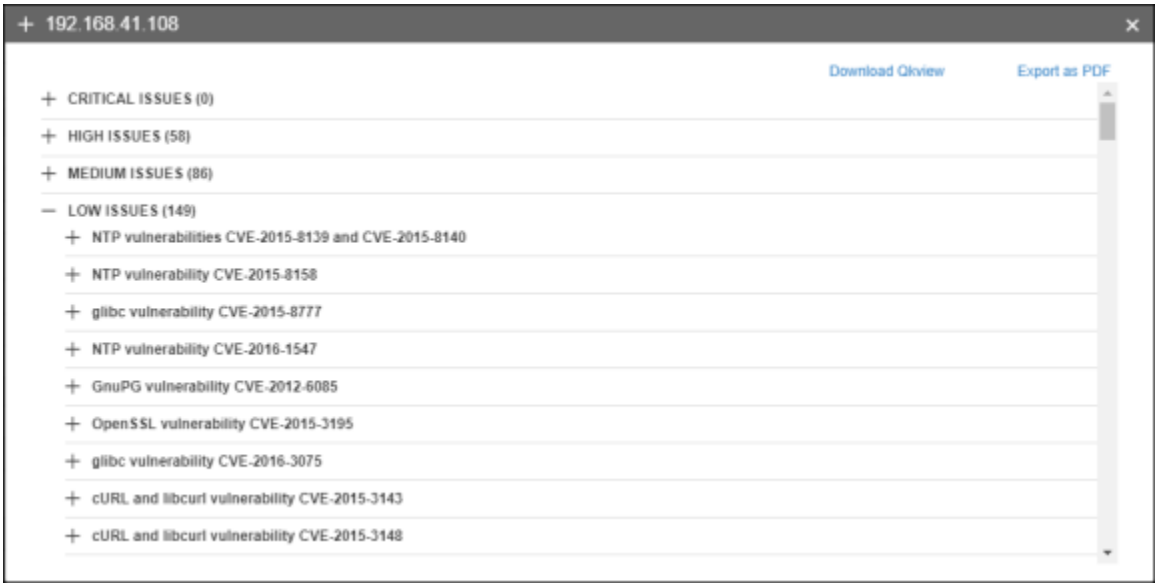
4. On the iHealth Report Generate screen that pops up, enter the case number for the report, then click Generate.
5. When the report is generated, it appears as a link in the Report column on the Device: ADC screen.
6. Click the IHEALTH_REPORT link.



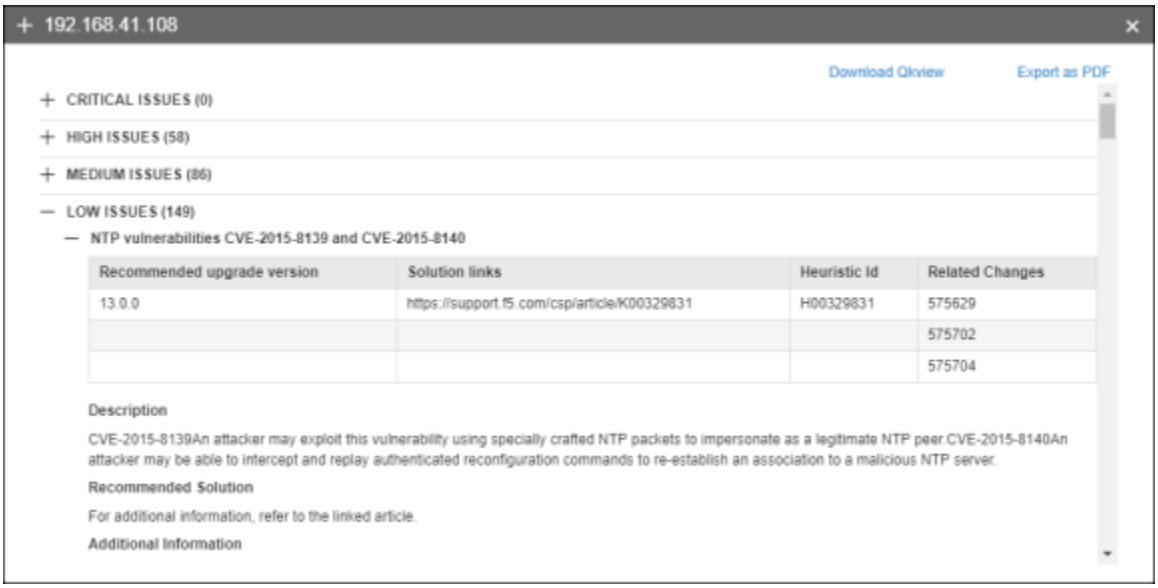
7. The iHealth report screen that pops up lists all of the current issues with the device, classified by their severity: critical, high, medium, or low.



8. Click any of the + (**Expand**) icons beside a severity level to view the issues within the corresponding category.



9. Within each severity level, click the name of a specific issue to view complete details, a recommended solution, and additional information about it.

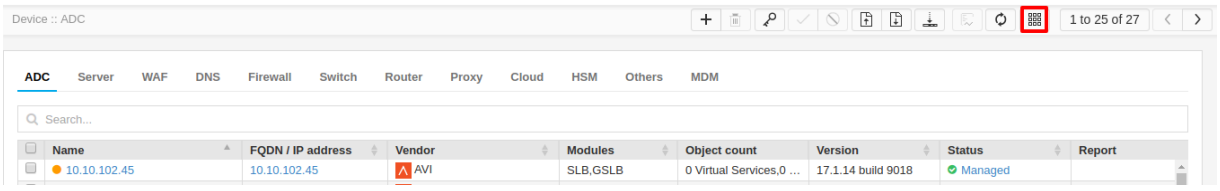


10. (Optional) Download the entire iHealth report as a Qkview file by clicking the **Download Qkview** link or as a PDF file by clicking the **Export as PDF** link, both of which appear in the top right corner of the screen.

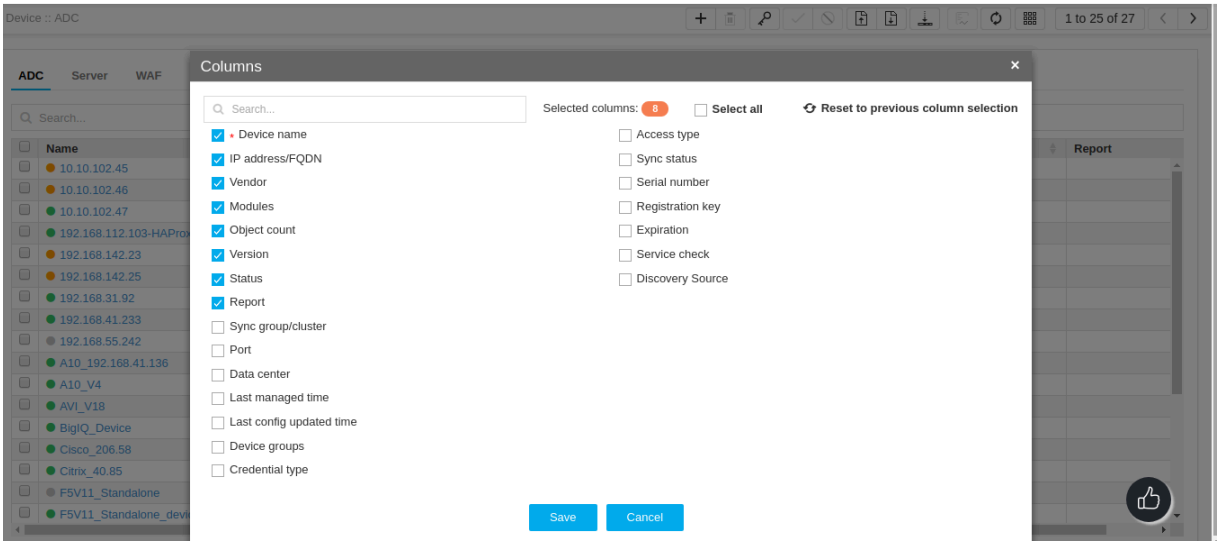
Selecting Inventory Columns

The user can select or unselect the list of columns to be displayed in the inventory page using this action.

1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Device**.
3. Click on the **Columns** icon.



4. In the popup window, select or unselect the columns to be displayed in the inventory page.

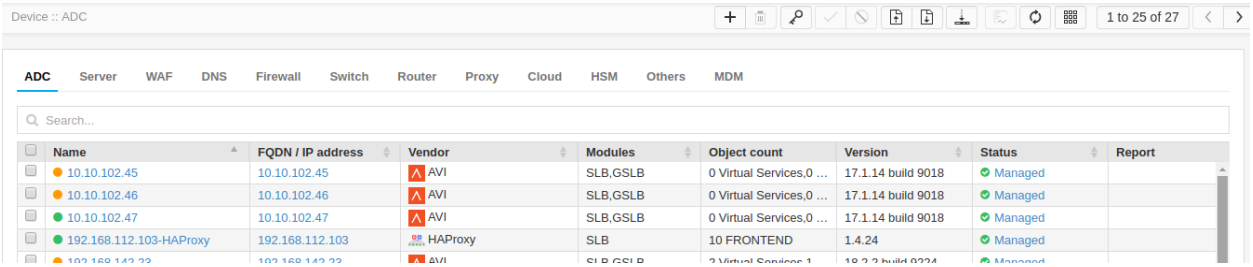


5. Click **Save**.

• Validating the column selection

Validating the column selection

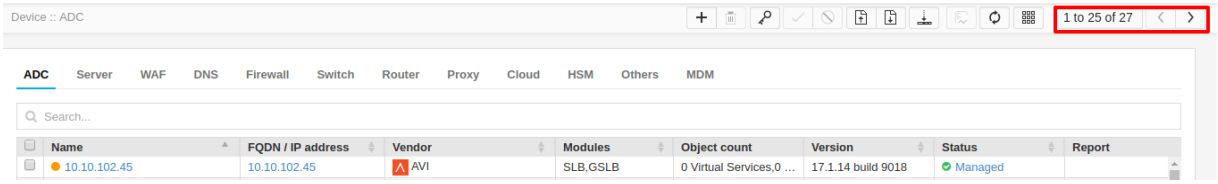
Once the user selects the columns to be displayed in the inventory page and saves the data, the device inventory page will be reloaded again with the selected columns.



Pagination

Pagination is being used to display many devices into the discrete pages. So The user can configure the number of device details to be displayed in a page and he can navigate to the previous and the next page using the previous and the next icon.

1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Device**.
3. Hover the mouse pointer over on the device count and select the number of records to be displayed in the device inventory page.



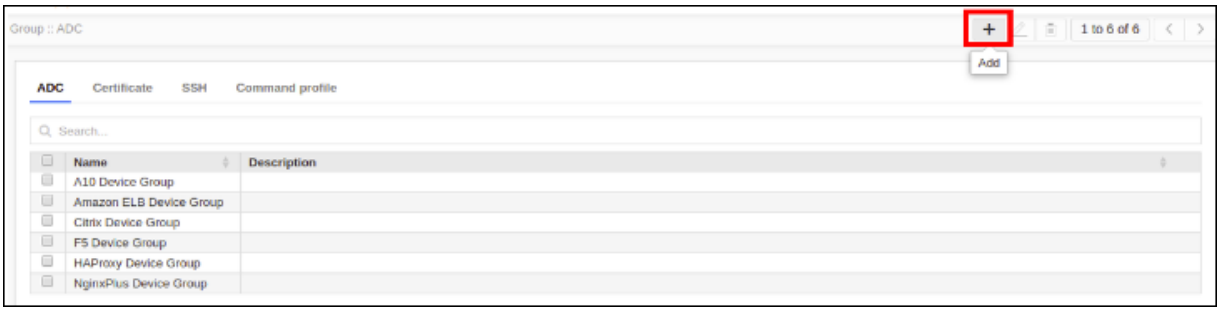
4. Select the Previous or Next icon to move to the previous or next page.

Chapter 4: Device Group

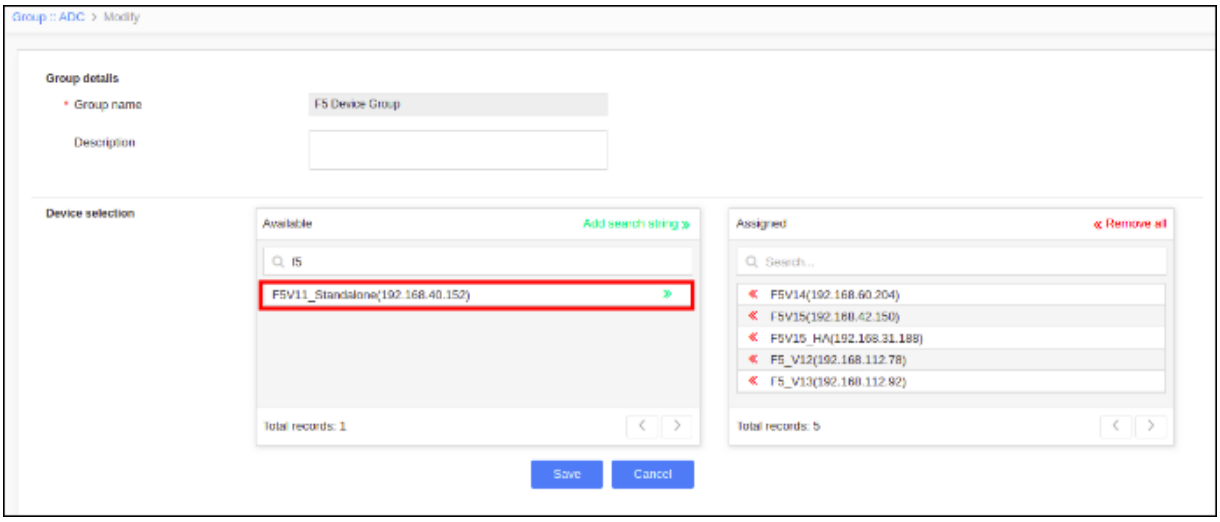
Device Group Addition

To add an ADC group to AppViewX:

1. Click the **Menu** > **ADC+** > **Asset Management** > **Device Group**.
   The **Group** screen opens.
2. In the **ADC** tab, click the + (**Add**) button in the Command bar.



3. On the **Add** screen, enter the name of the new group. (Recommended) Enter a description of the group to help users identify it.
4. In the Device selection field, click the » (**Assign item**) icon beside each device you want to include in the group.



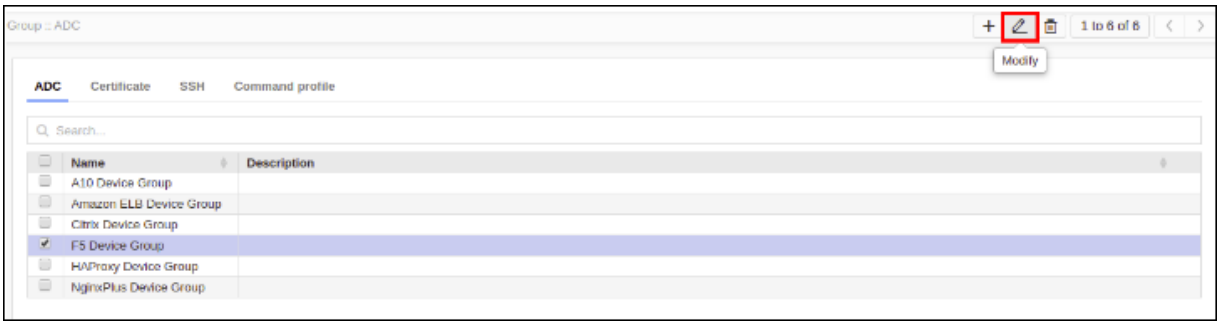
5. When you have finished assigning devices to the group, click **Save** to add them to the system.

> **Note:** Rather than adding devices manually, you can click the Add search string link and create a search string that automatically assigns all existing devices that match the filter criteria to the ADC group. The benefit of using a search string rather than selecting devices manually is that the search string continues to work in the background, auto-assigning all new devices to the ADC group if the devices match the search criteria you set up.

Device Group Modification

To modify an ADC group to AppViewX:

1. Click the **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Group**.
   The **Group** screen opens.
2. If the ADC group whose details you want to modify is not displayed on the screen, use the search field to locate it.
3. In the **ADC** tab, select the checkbox beside the name of the ADC group.
4. Click the **Modify** button in the Command bar.

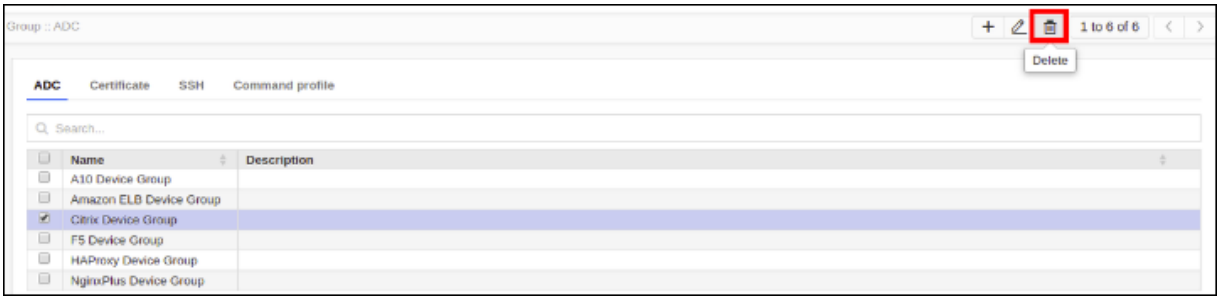


5. On the Modify screen that appears, make whatever changes you want to the content.
6. Click **Update** to save your changes.

Device Group Deletion

To delete an ADC group to AppViewX:

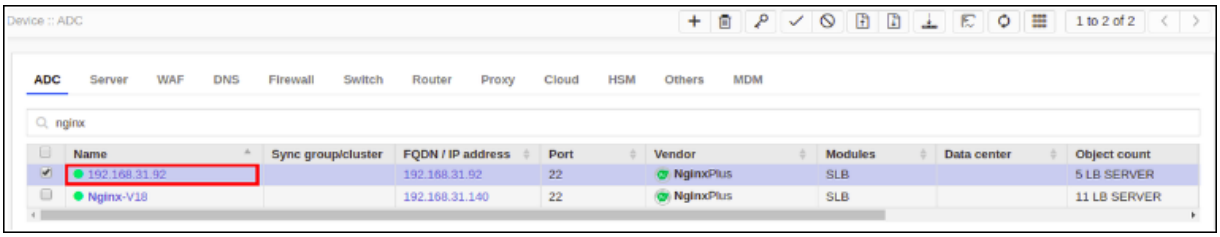
1. Click the **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Group**.
   The Group screen opens.
2. Select the checkbox beside the group you want to delete.
3. Click the (**Delete**) button in the Command bar.



4. On the confirmation screen that pops up asking you if you are sure you want to proceed, click **Yes**.
5. The group is then removed from the AppViewX system.

Assign a Device to Group(s)

1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Device**.
3. Search for the device to be added to device group(s) and select the respective device and navigate to the **Device group** page.

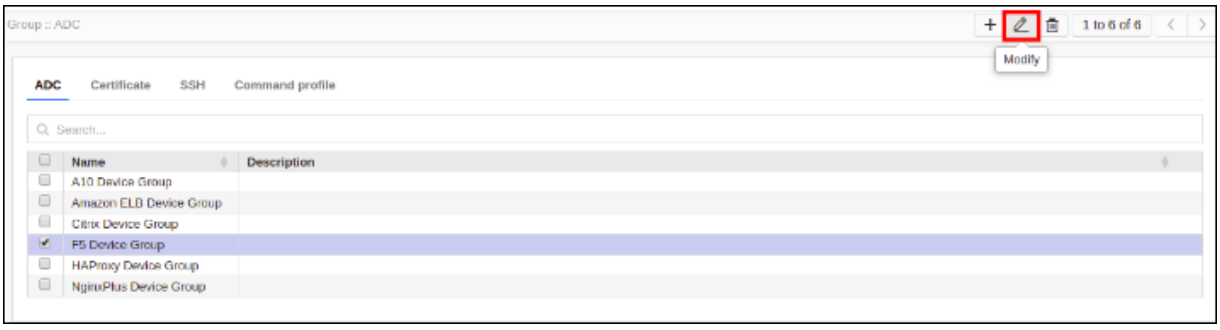


4. Select the device group(s).

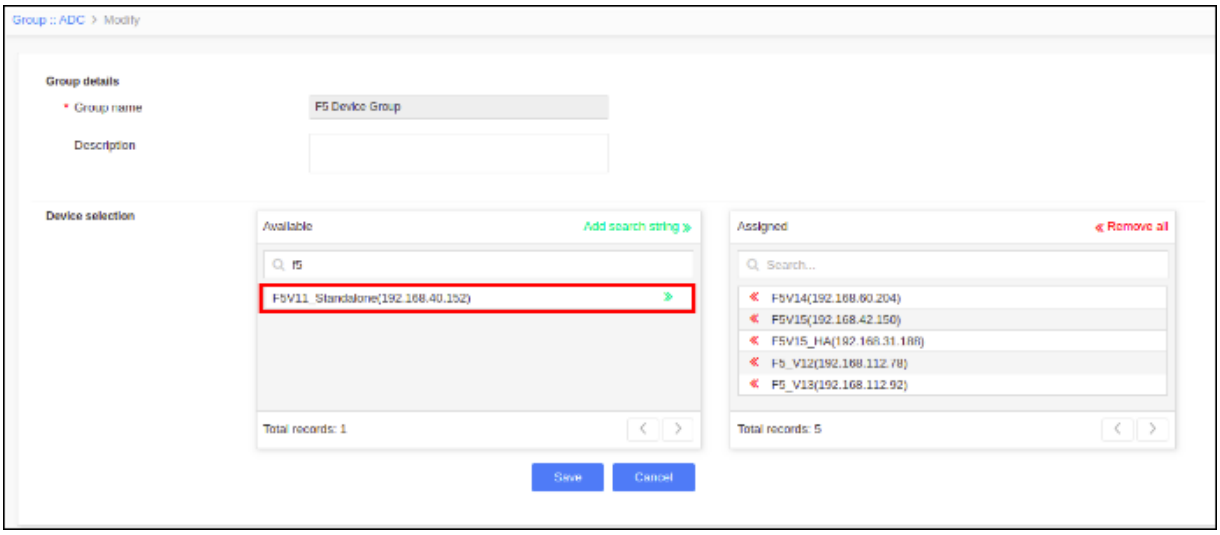
5. Click **Save**.

Assign/unassign devices

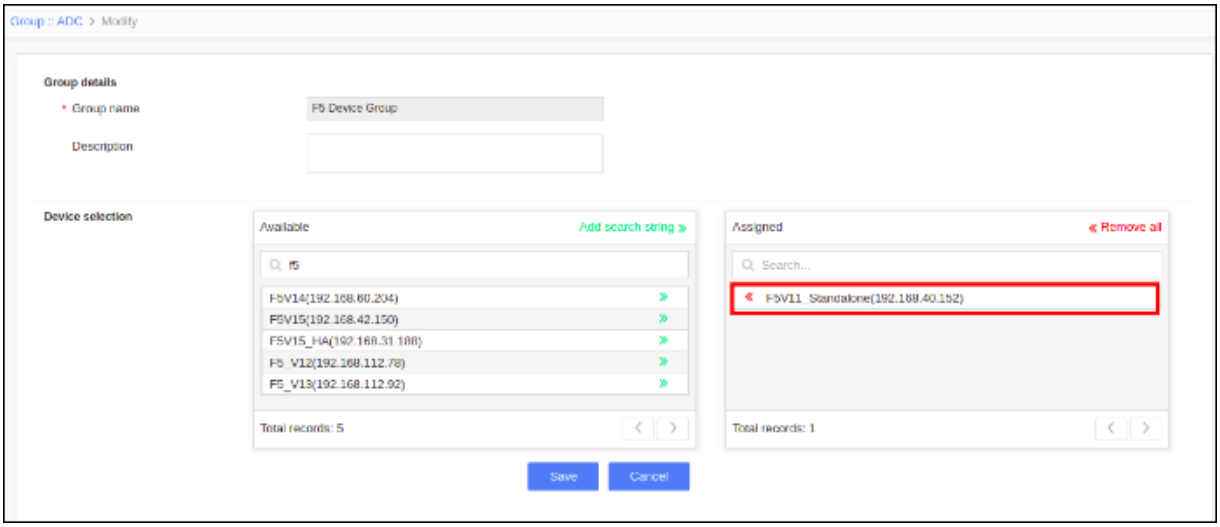
1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Group**.
3. From the **Group** page, select the device group to be modified and click the **Modify** icon to navigate to the Group Modification page.



4. To assign devices in the group, search for the device and select the devices under the **Available** list.



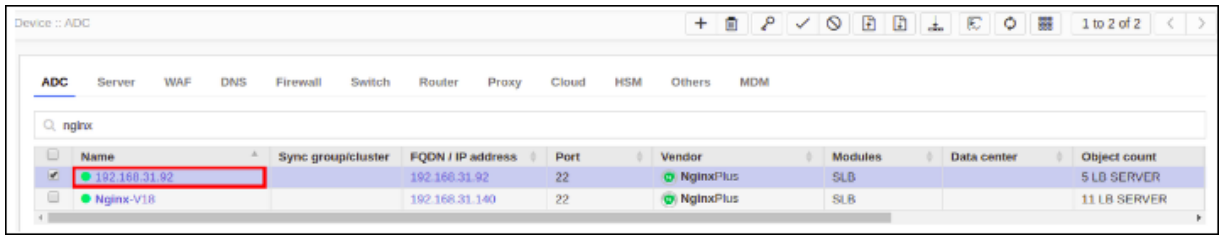
5. To unassign devices in the group, search for the device and select the devices under the **Assigned** list.



6. Click **Save**.

Unassign a Device from Group(s)

1. Login to the AppViewX application with valid credentials.
2. Select **Menu** > **Inventory** > **Device**.
3. Search for the device to be removed from device group(s) and select the respective device and navigate to the **Device group** page.



4. Unselect the device group(s).

5. Click **Save**.

Chapter 5: Backup and restore

Backup and Restore

Configuring devices for Backup and Restore required the users to have added the devices whose backup is to be taken in the Inventory.

User should also have the ACF permission for Backup and restore.

Vendors Supported in AppViewX for BackUp

Vendors	BackUp	Restore
F5	Device	Device & Object
Citrix	Device	Device & Object
A10	Device	Device & Object
Avi	Device	Device

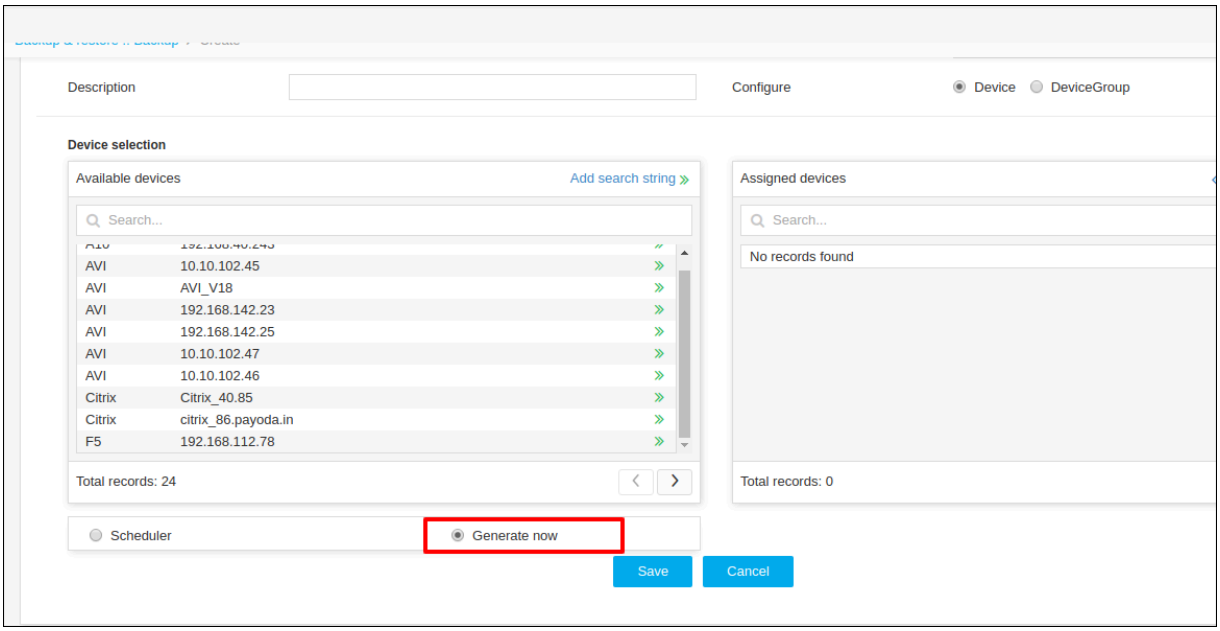
Configuring Device Backup

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu ->Inventory -> BackUp&Restore.**
3. Click on the Add **(+)** icon to navigate to the BackUp configuration page

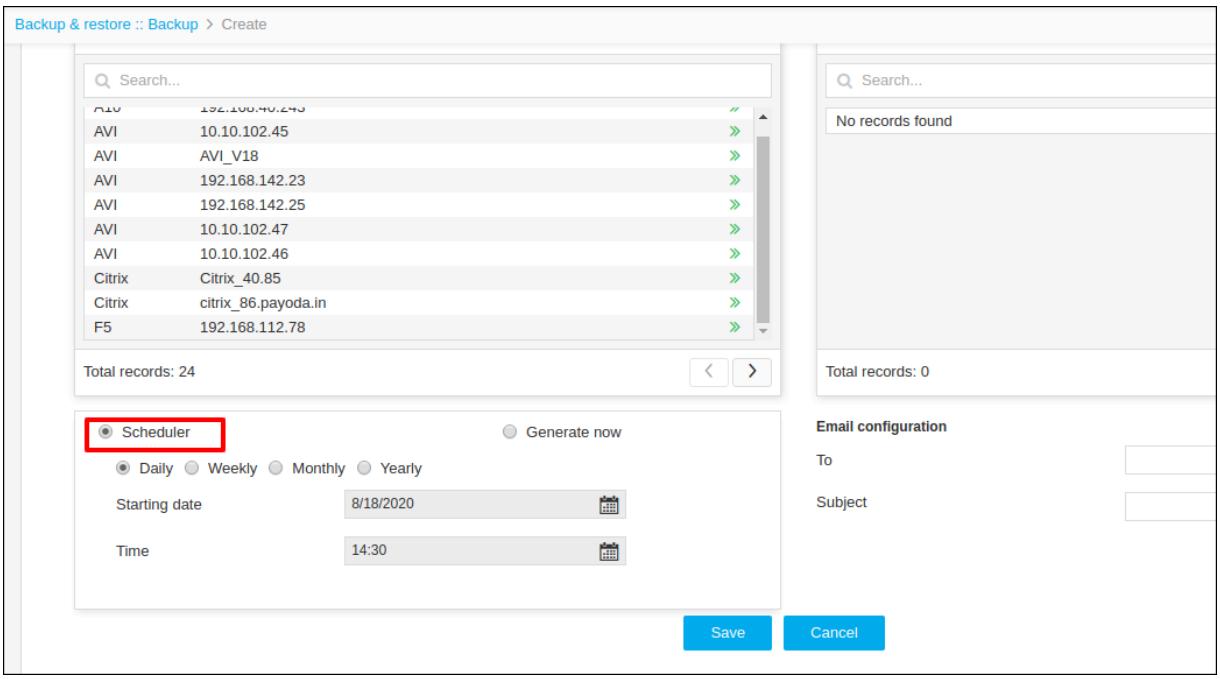
4. Users can select individual devices or device groups for BackUp
5. Provide the required details

Name	Type	Mandatory	Description
Device Type	Text	Yes	Type of device to be selected (ADC,Proxy,WAF,Firewall)
BackUp Name	Text	Yes	BackUp name accepts only alphanumeric characters, '-' , '_' , '.'. Also should not start or end with a special character.
Description	Text	No	NA
Configure	Radio Button	Yes	Device or Device Group
Device or Device Group selection	Search Box and select from the search window	Yes	NA
Scheduler/ Generate now	Radio Button	Yes	NA
Email configuration to	Text box	No	NA
Email configuration subject	Text box	No	NA

6. Schedule the BackUp by clicking Scheduler or Generate now.



7. Users can select the scheduler on Daily/Weekly/Monthly or Yearly basis and provide the date and time appropriately.

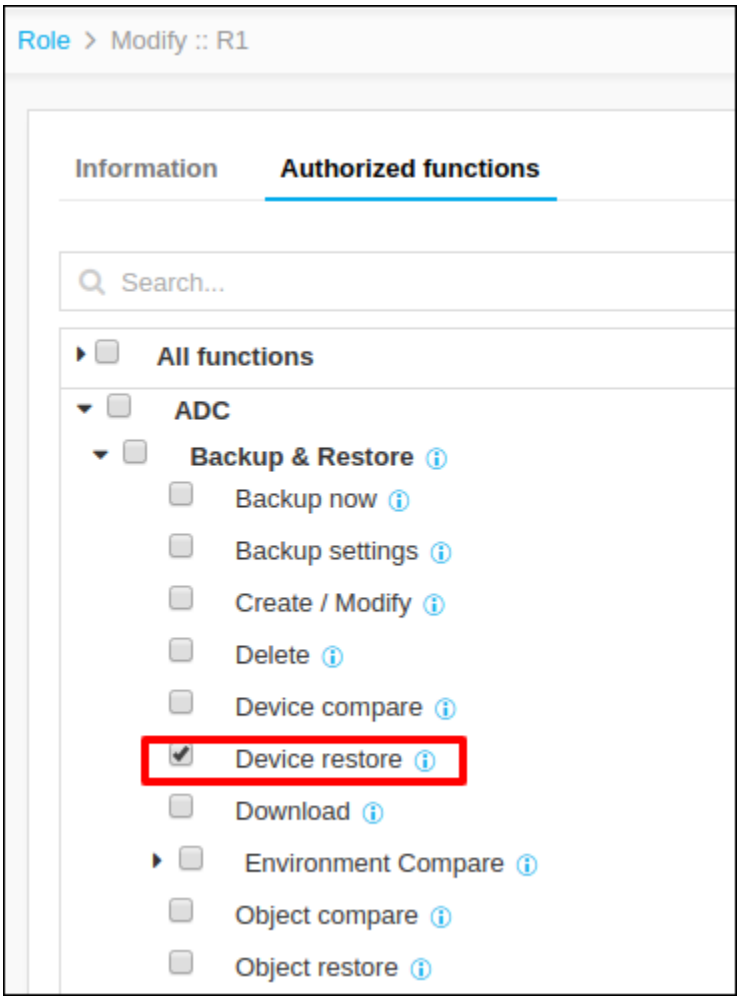


8. Click **Save**
9. To view BackUps generated in a particular group, click on the (+) icon on the tab that has the backup group name.

10. To edit the already created BackUp group, click on the pencil icon on the tab mentioned with the backup group name.

Restore from Backup

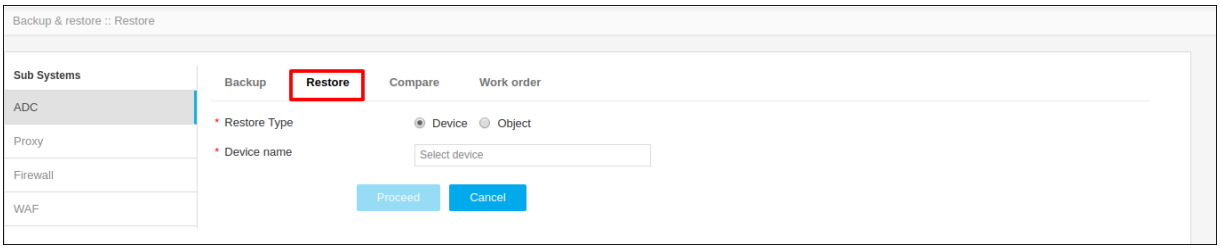
Users can restore the device/objects added in AppViewX from the Backup generated. The users should have ACF permission for Restore and ACL permission on those devices for which restore has to be performed.



• Restore Device/Object with the Backup Generated

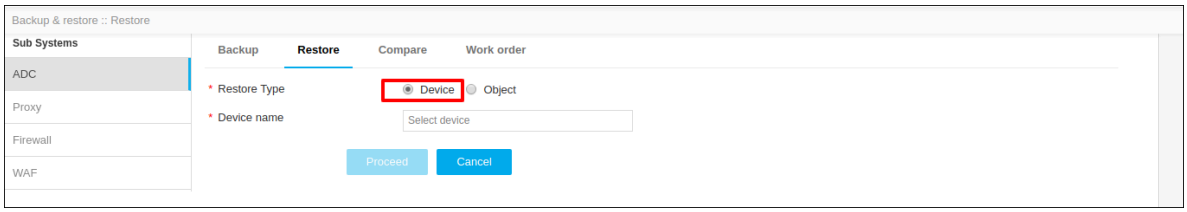
Restore Device/Object with the Backup Generated

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu ->Inventory -> BackUp&Restore**.
3. Click on the Restore tab to navigate to the Restore page.



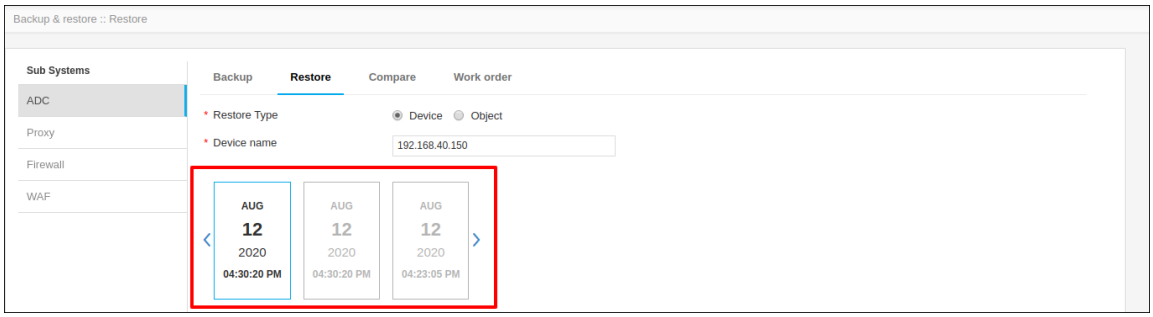
4. Click on the Device/Object that needs to be restored.

a. **Device Restore:**



i. Provide the device name whose backup is to be restored in the Device Name text box.

ii. All the Backups generated for this particular device will be listed below.

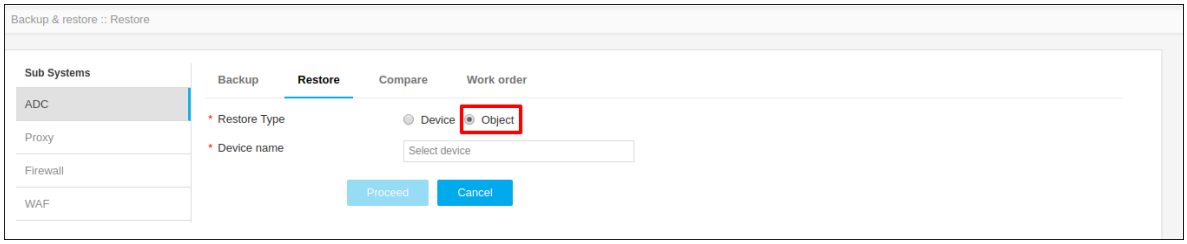


iii. Select which backup to be used and provide the device name to which the restore needs to be performed.

iv. Click Proceed to navigate to the next page, where the Reason for restore is to be provided.

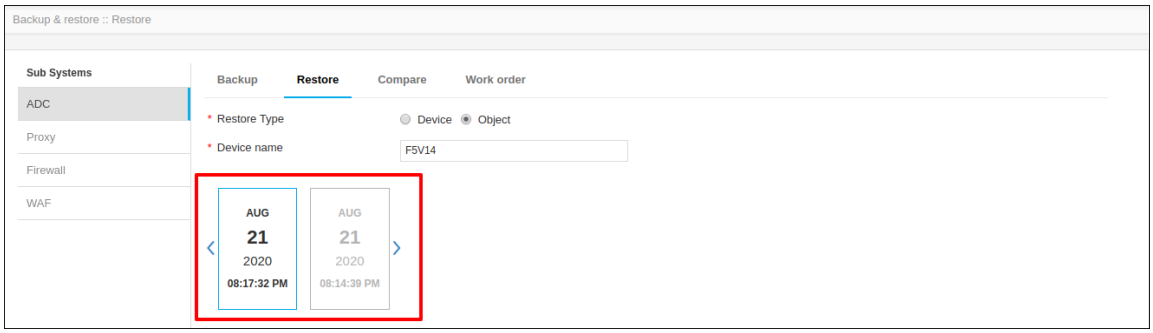
v. Click Restore.

b. **Object Restore:**



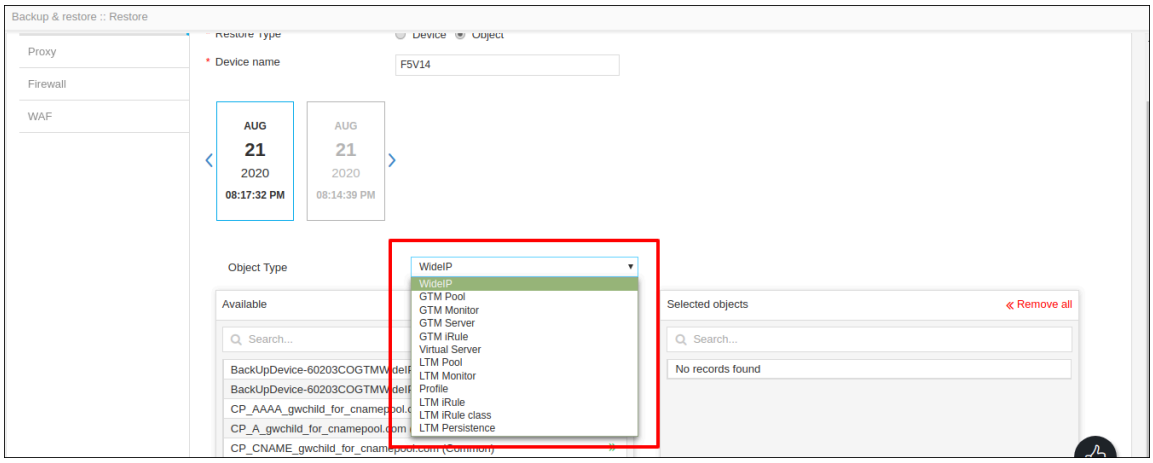
i. Provide the device name whose object is to be taken for restore in the Device Name text box.

ii. All the Backups generated for this particular device will be listed below.



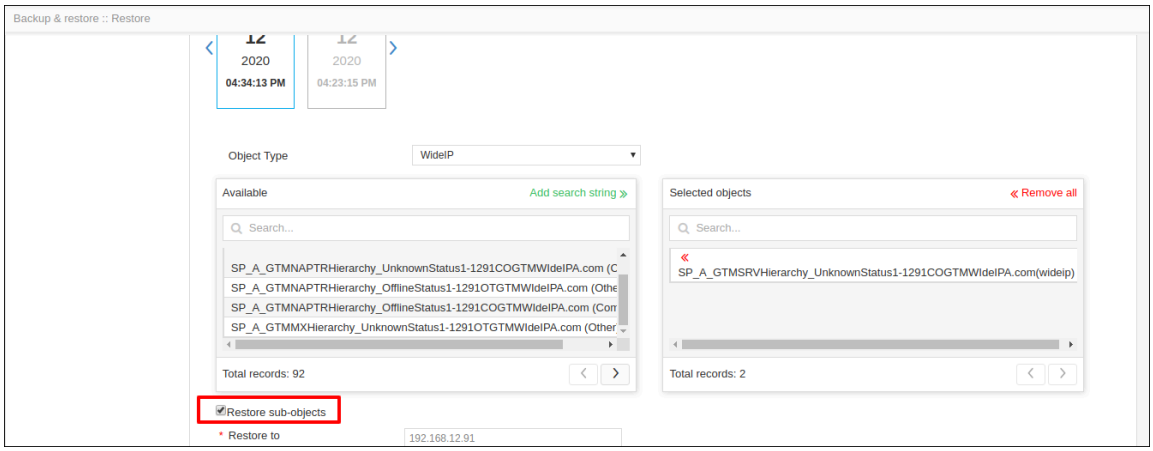
iii. Select which backup to be used for restoring the object.

iv. Select which type of object is to be restored by clicking on the drop down menu for Object Type.



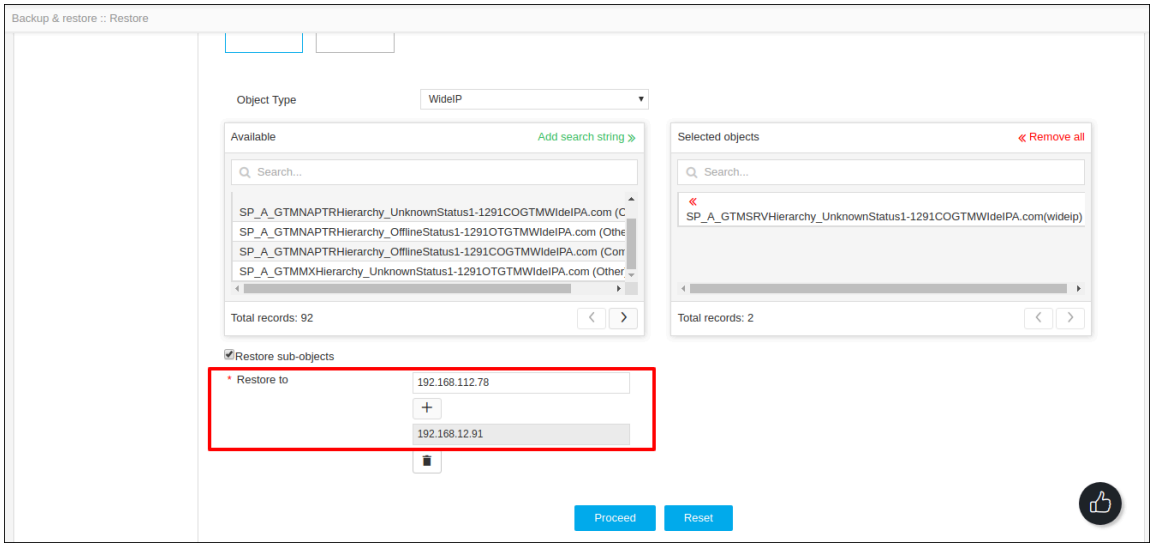
v. All the objects pertaining to the selected object type will be listed below. Users can select which all objects to be restored by moving the objects from the available object list to selected object list.

vi. If the restore needs to be performed on sub-objects as well, then the user can check the checkbox provided to Restore sub-objects.



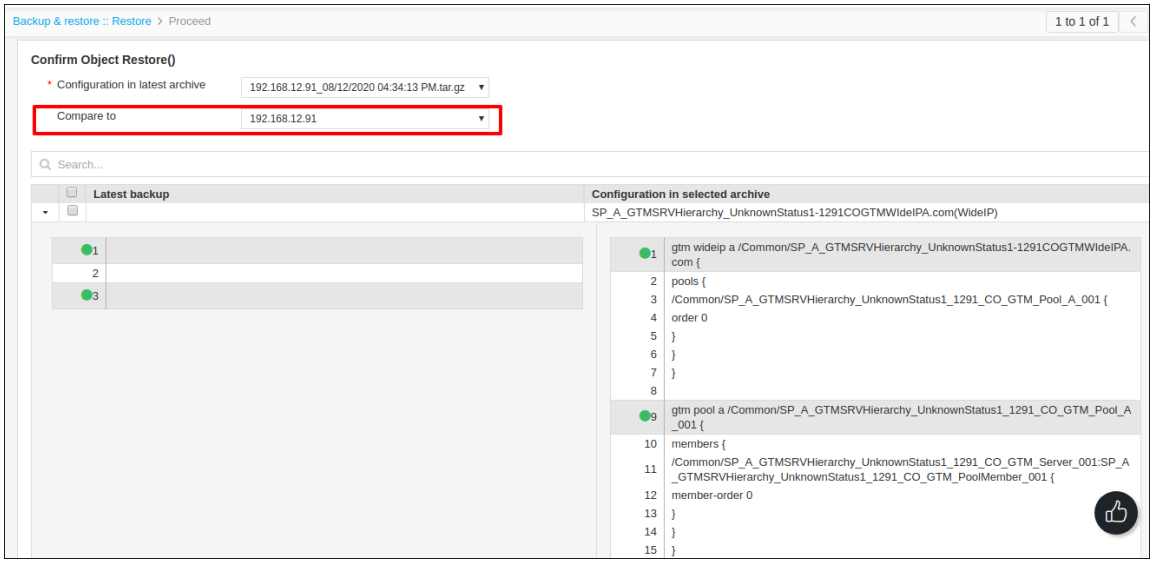
vii. Provide the device name to which the back up objects need to be restored.

viii. Users can restore an object to a single/many devices. Restoring more than one device can be done by clicking (+) sign and providing the device name.

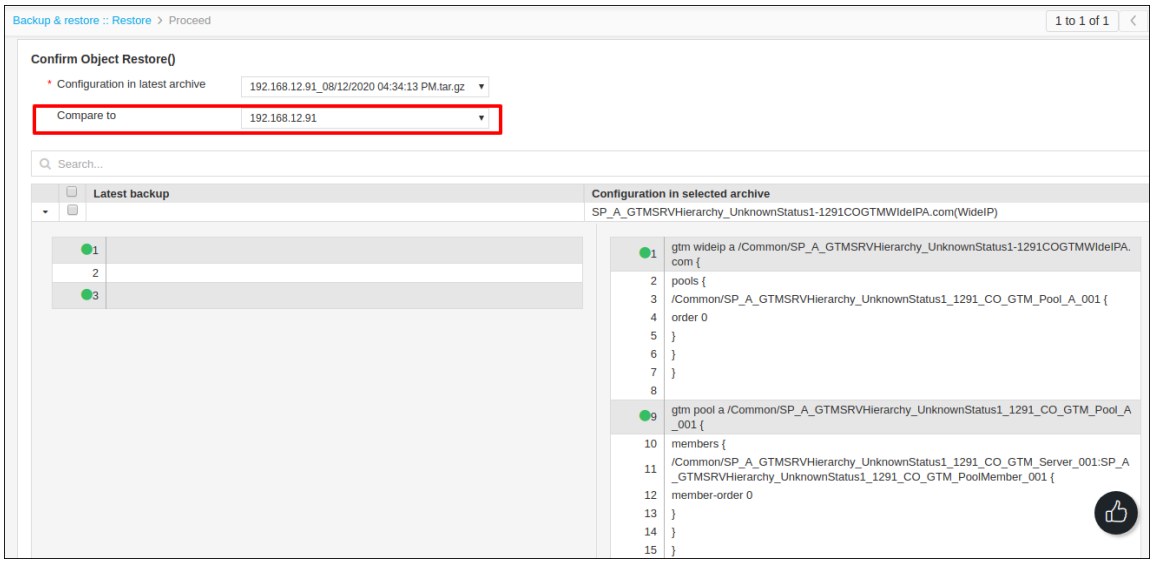


ix. Click proceed to navigate to the next page where Confirmation to Object Restore is requested.

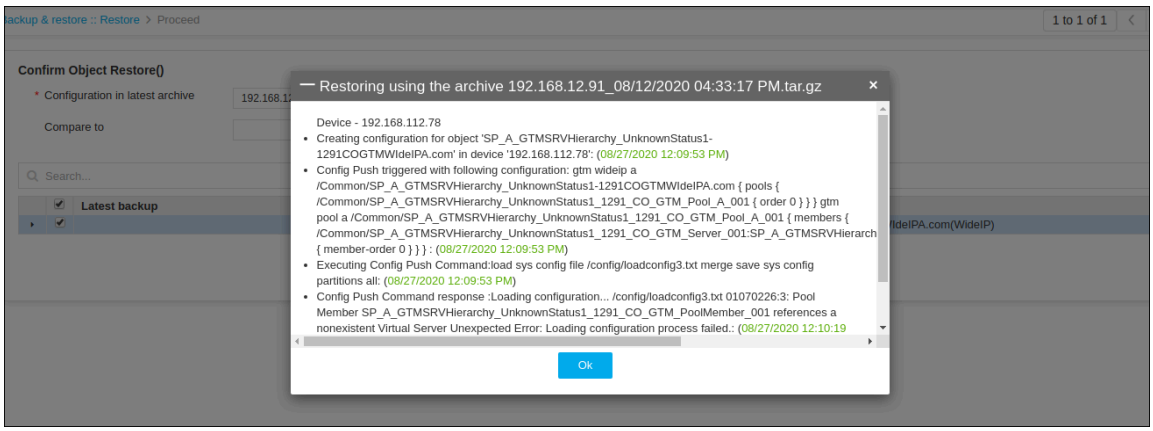
x. Users can check or compare the configuration of objects from the back up and the current object and cross verify the same.



xi. Provide the reason for restore and click Restore all.



xii. Users can view the restore success message on the screen once restore is successful.

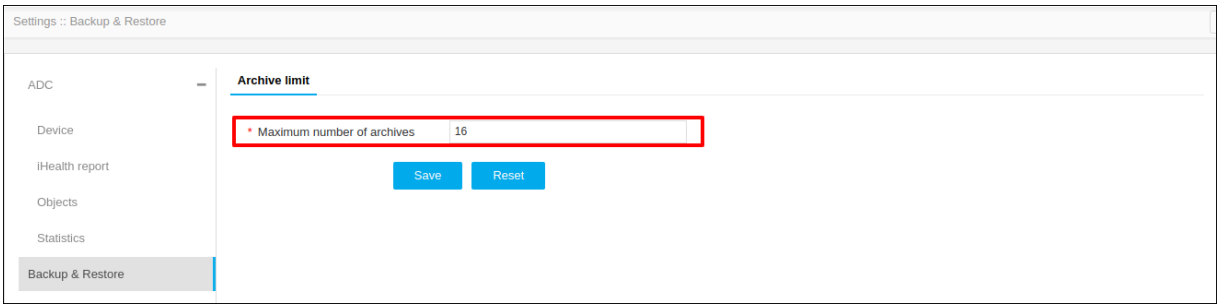


Configuring Backup Settings

To configure Backup & Restore settings, the user should have ACF permissions to Backup settings.

Configuring the Maximum Number of Archives Saved

1. Log in to the AppViewX application with valid credentials
2. Select **Menu -> Settings -> ADC -> Backup & Restore.**
3. Enter the maximum number of archives to be stored in AppViewX in Maximum number of archives test box. The default value will be 16.

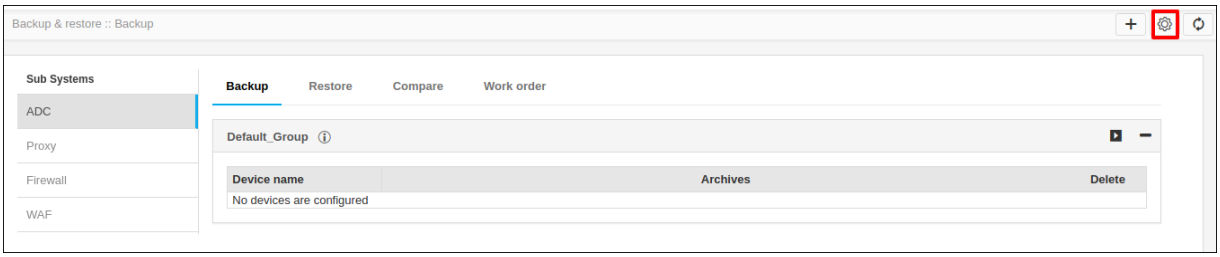


4. Click **Save**

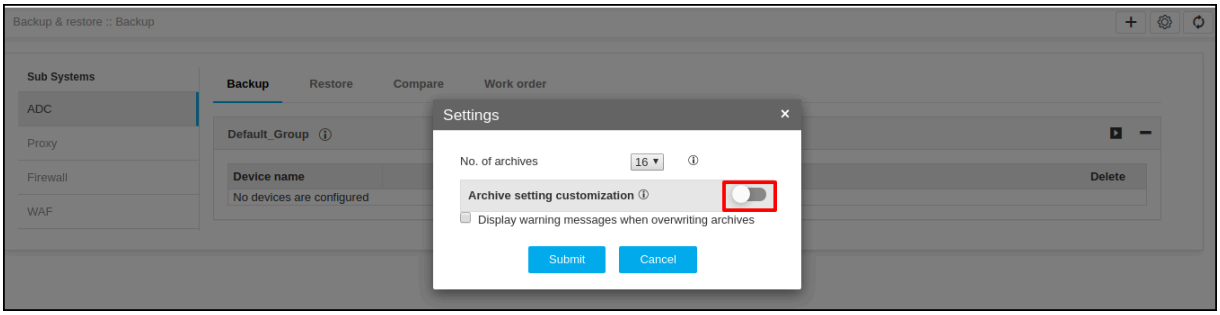
Archive Setting Customization

Users can customize the number of archives stored for devices based on daily/weekly/monthly/yearly.

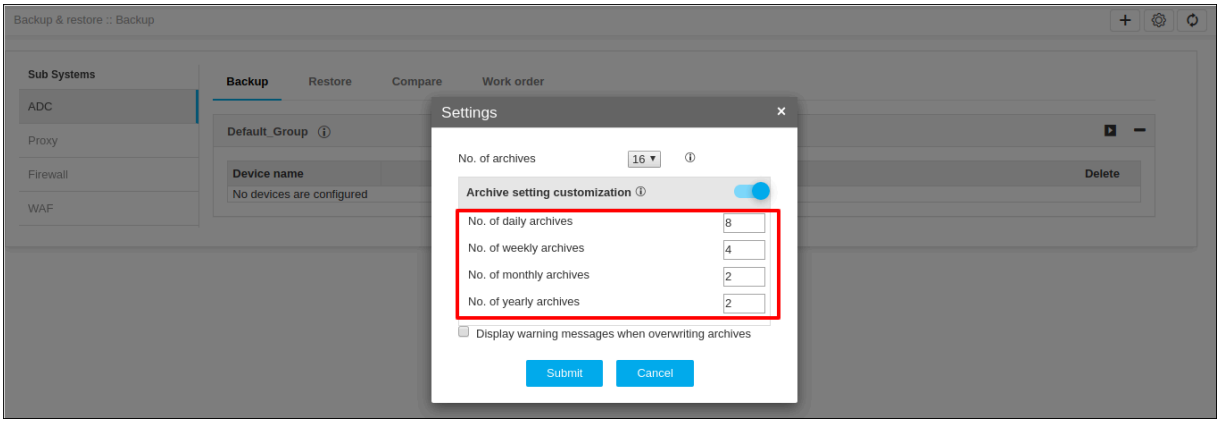
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu ->Inventory -> BackUp&Restore.**
3. Click on the Settings icon on the top right corner.



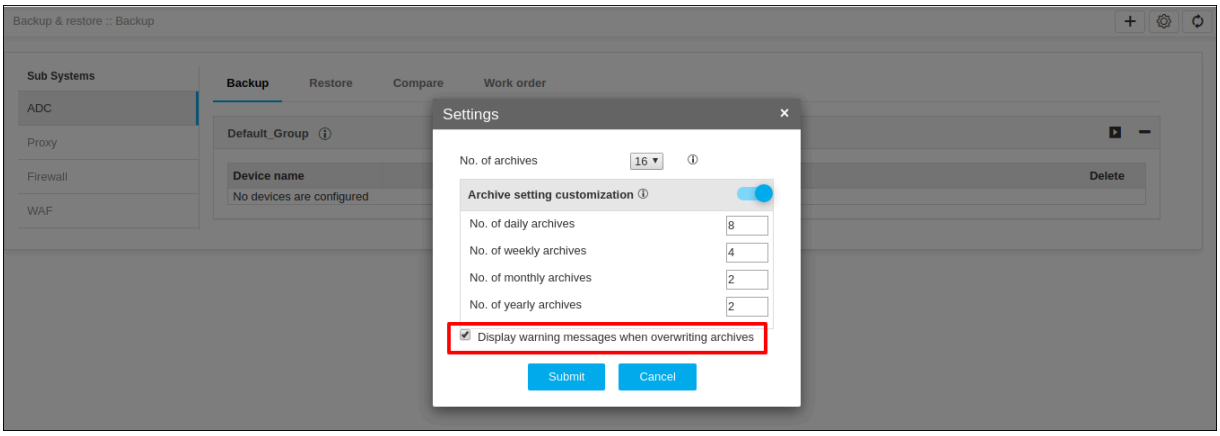
4. Enable the Archive setting customization button.



5. Here the users can provide how many archives are to be stored for devices on a daily/weekly/monthly/ yearly basis.



6. Users also can enable the radio button to display the warning message when archives are overridden. Enabling this will show a pop up if the number of archives configured by the user causes any removal/ deletion of archives.

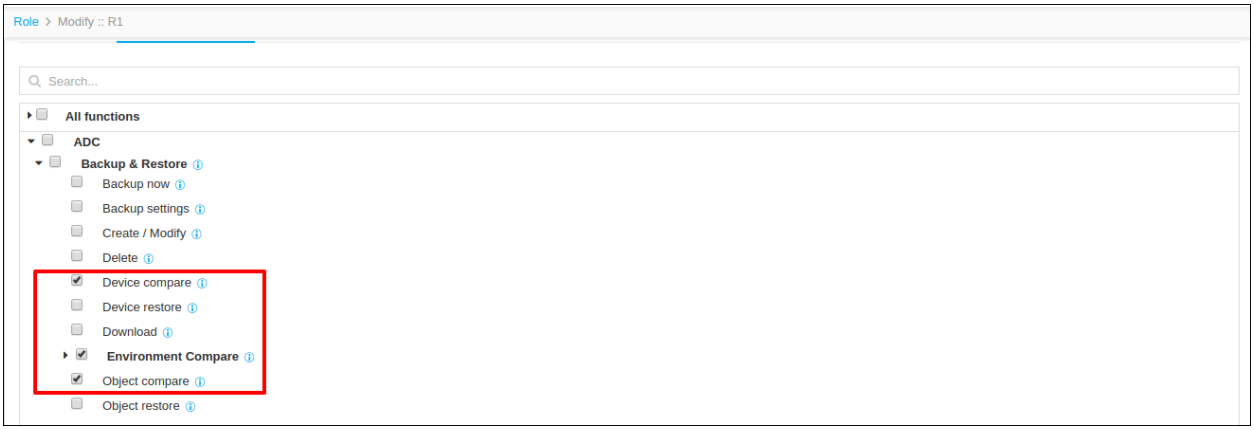


7. Click Submit.

Compare Backup

Users can compare between 2 archives generated. They can compare between both the devices as well as objects.

To compare the backup, the user should have ACF permissions to Device compare, Object compare and environment compare.

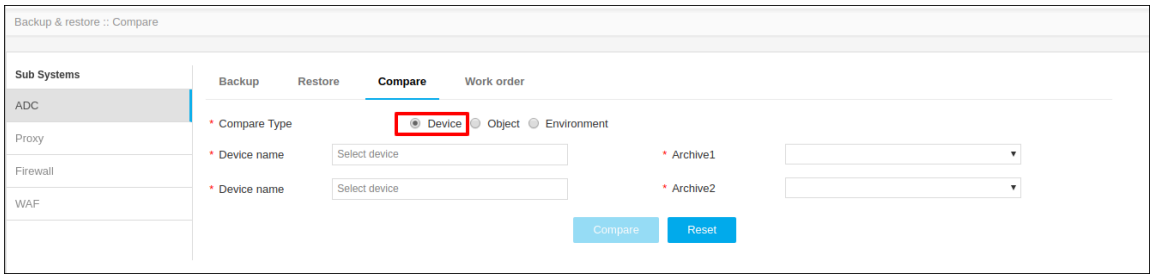


Comparing Between Two Backup Generated

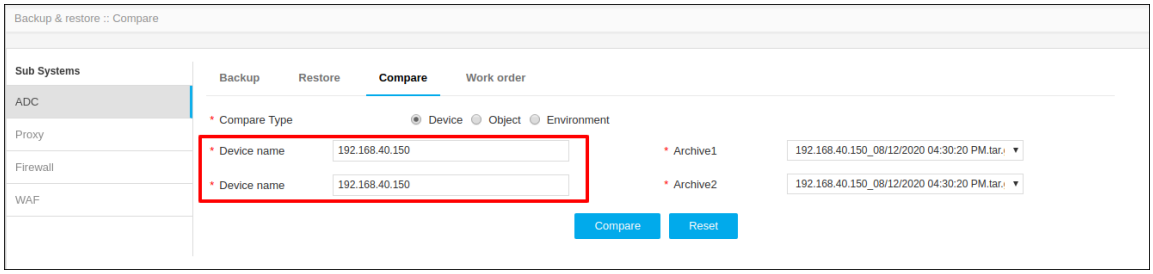
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu ->Inventory -> BackUp&Restore**.
3. Click on the Compare tab to navigate to the Restore page.

a. **Device compare:**

i. Select the **Device** radio button in Compare type.

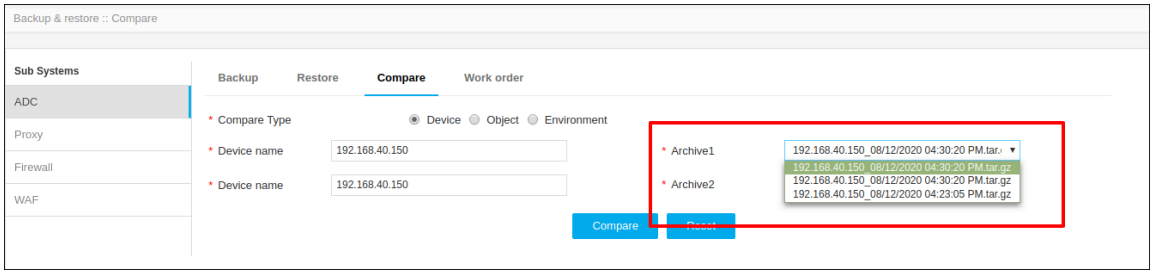


ii. Provide the device names across which the backup is to be compared. Users can compare the backup between the same devices or different devices as well.



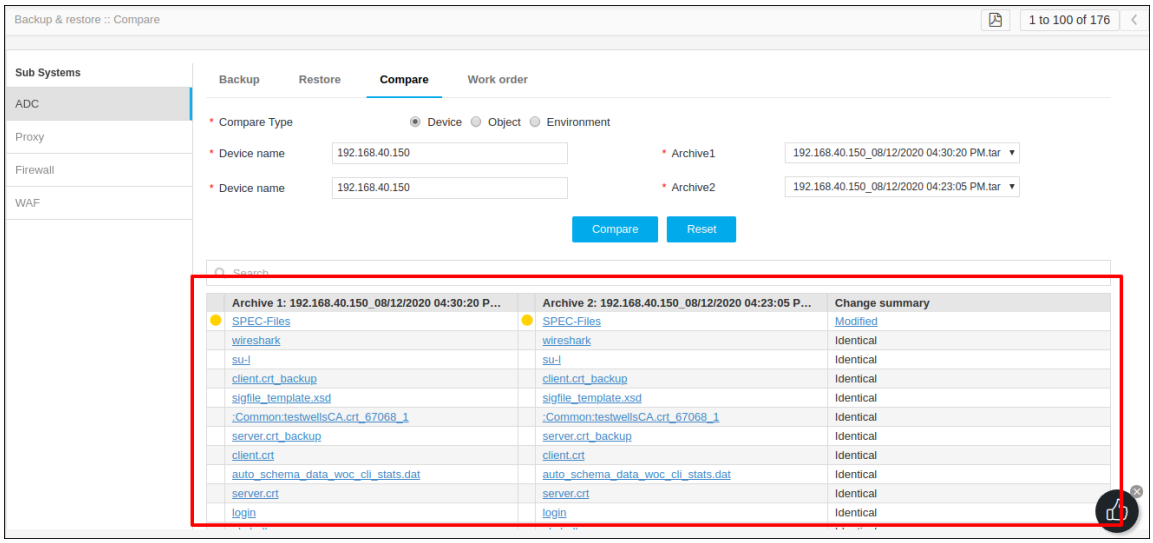
iii. After the device is selected, the backups generated for that particular device will be brought up in the archive list.

iv. Select which archive is to be compared from the drop down list.



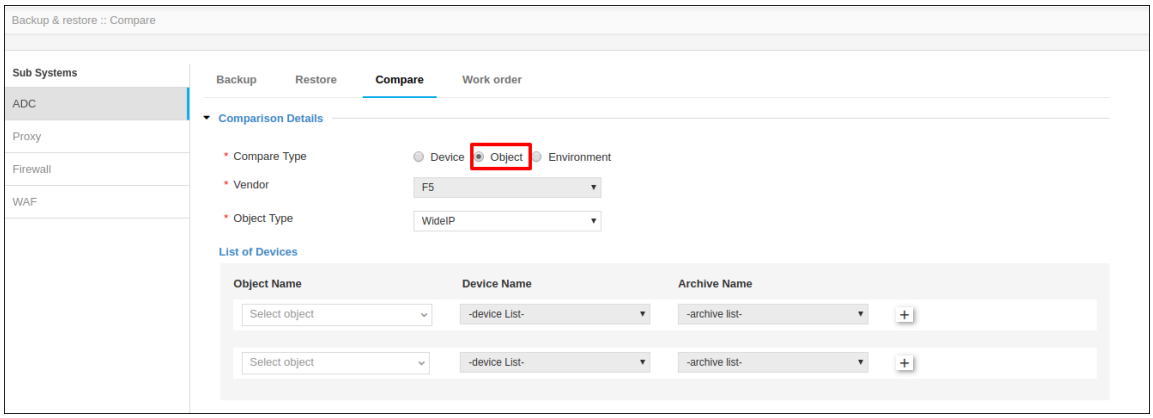
v. Click Compare

vi. The two archives along with the change summary will be displayed in the same page below.



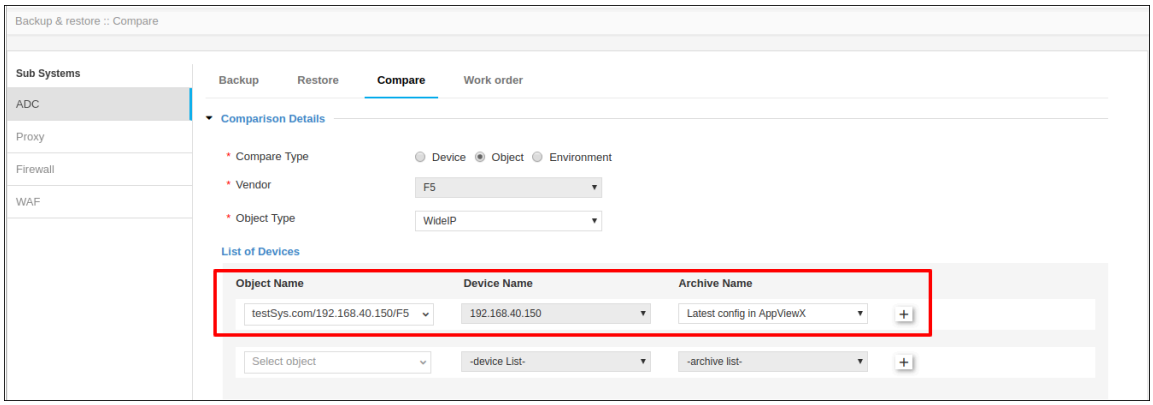
b. **Object compare:**

i. Select the **Object** radio button in Compare type.



ii. Select the Vendor and Object type to be compared from the drop down menu.

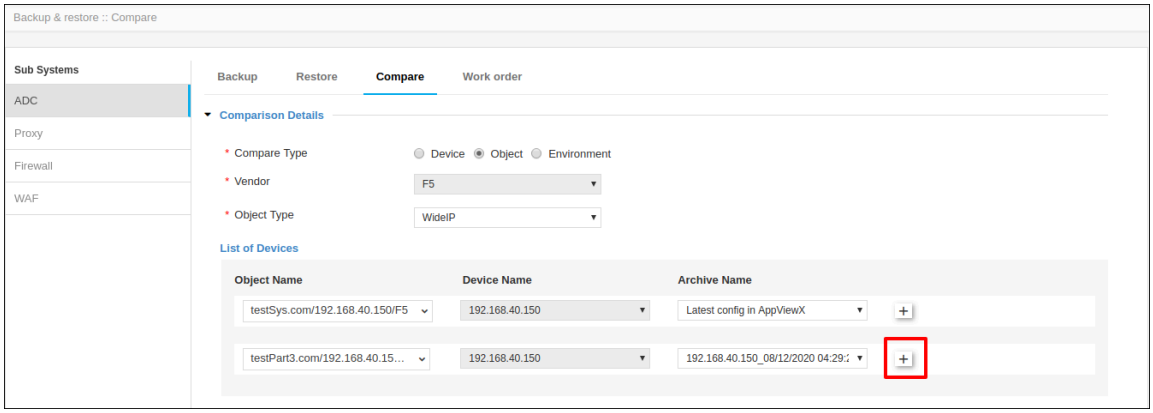
iii. Select the object name to be compared from the drop down menu of Object Name. This will automatically populate the device name tab corresponding to this object.



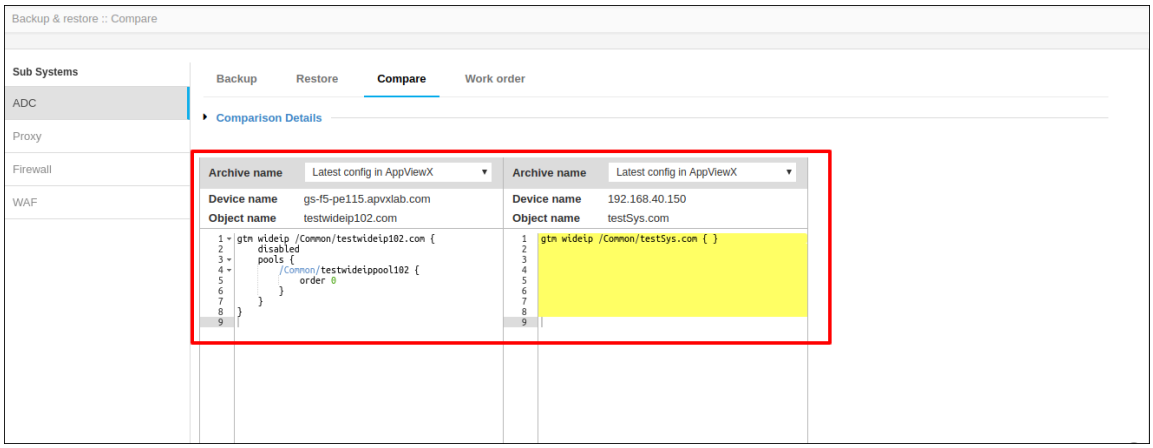
iv. From the menu of Archive names, select which archive to be compared. Users can either select the latest archive generated or select any of the archives generated earlier for the object.

v. Similarly users can add other objects to be compared.

vi. Users can add more than 2 objects to be compared by clicking the (+) icon near the Archive names. Users can add maximum of 5 objects to compare.



vii. Click Compare.


Backup & restore :: Compare
Sub Systems
ADC
Proxy
Firewall
WAF
Backup
Restore
Compare
Work order
Comparison Details
Archive name
Latest config in AppViewX
Device name
gs-f5-pe115.apvxlab.com
Object name
testwideip102.com
gtm wideip /Common/testwideip102.com {
disabled
pools {
/Common/testwideippool102 {
order 0
}
}
}
Archive name
Latest config in AppViewX
Device name
192.168.40.150
Object name
testSys.com
gtm wideip /Common/testSys.com { }

4.

Chapter 6: Role Based Access Conrol

RBAC Configuration

Role Based Access Control (RBAC)

Role based access control (RBAC) is a method of restricting AppViewX functions, network resources which can be managed and monitored in AppViewX based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the AppViewX functions and network resources they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Benefits of RBAC

Using RBAC should improve operational efficiency, enhance compliance, provide administrators increased visibility, reduction in costs, decrease in risk of breaches and data leakage.

Simplified RBAC Configuration in AppViewX

To simplify existing RBAC Configuration in AppViewX for the Account Administrator, “Quick Config” wizard flow option has been introduced in the existing Authentication, User groups, Roles and Resources. Using “Quick Config” option, users should be able to perform all the following actions in the same wizard flow:

- Configure external authentication or single-sign on for users to login to AppViewX
- Add users groups into AppViewX by pulling specific user groups from AD into AppViewX based on specific patterns/keywords/codes and support Bulk Export/Import option to onboard user groups
- Pre-packaged roles for ADC, Cert, Security and Automation modules to assign permissions to user groups

- Simplifying custom role creation by providing information help against each ACF explaining the significance of the functionality
- Dynamic rule based resource tagging of newly discovered ADC objects, Certificates based on Query or using script and assigning permissions to user groups dynamically.

Accessing Quick Config option

To configure RBAC using Quick Config option,

- Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config** option.
- The Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of the wizard flow, user groups, roles, and resources stages are displayed at the top. Click on the respective stage for configuration.

Ways to Access Quick Config Wizard Flow

- Click **Menu** > **Account** > **User group** > **Quick Config** option.

(or)

- Click **Account** > **Role** > **Quick Config** option

(or)

- Click **Account** > **Resource** > **Quick Config** option.

The Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of the wizard flow, user groups, roles, and resources stages are displayed at the top. Click on the respective stage for configuration.

For detailed instructions to perform the above-mentioned actions, see Platform User Guide.

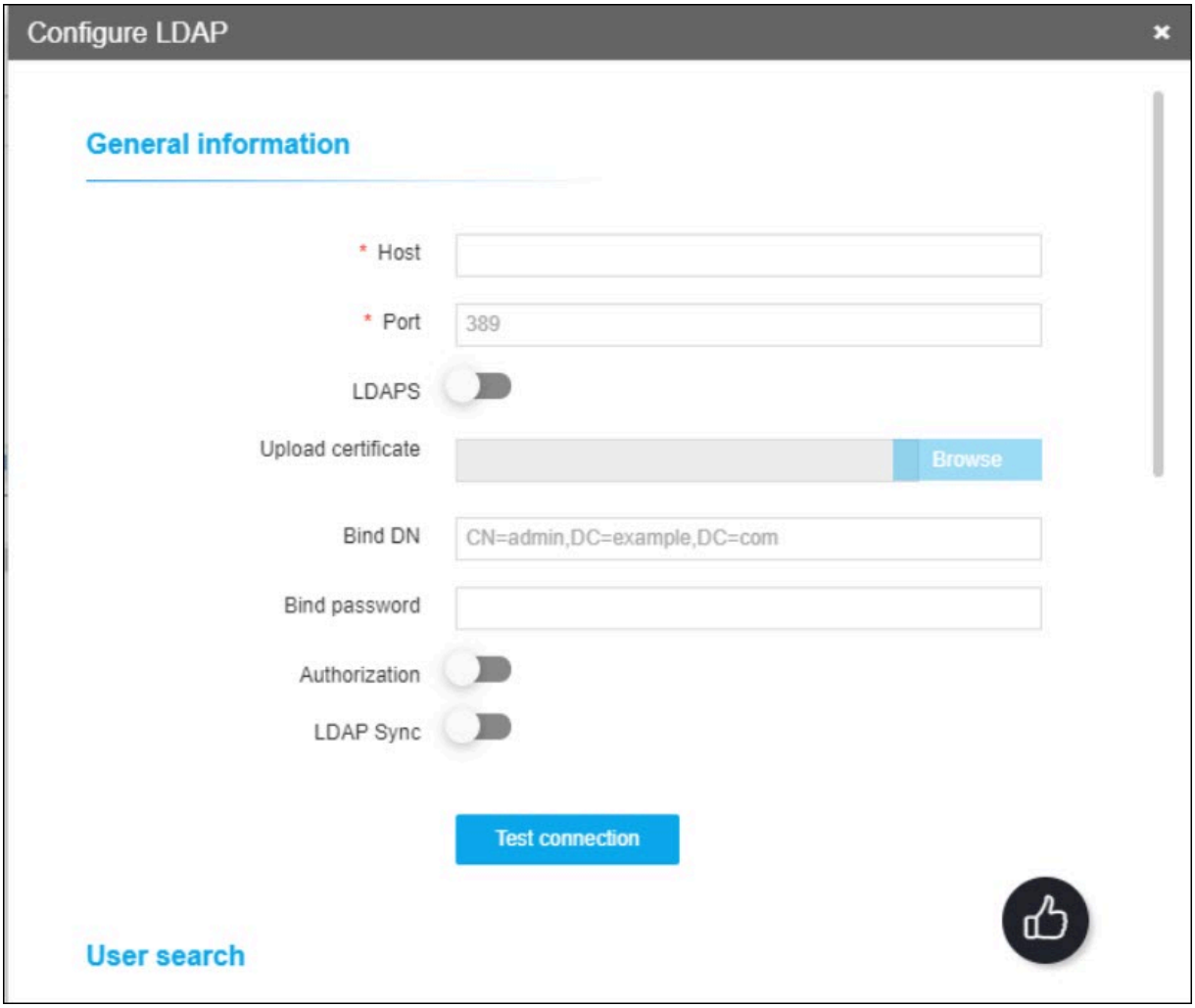
Authentication

The Quick Config option in Authentication sub-tab within the Settings > General tab enables you to configure and manage authentication for Lightweight Directory Access Protocol (LDAP), LDAPS (LDAP over SSL), TACACS, RADIUS, and Single-Sign on accounts. It also allows you to set the order levels for the three different types of authentication and to restrict users to a single session, if necessary.

LDAP

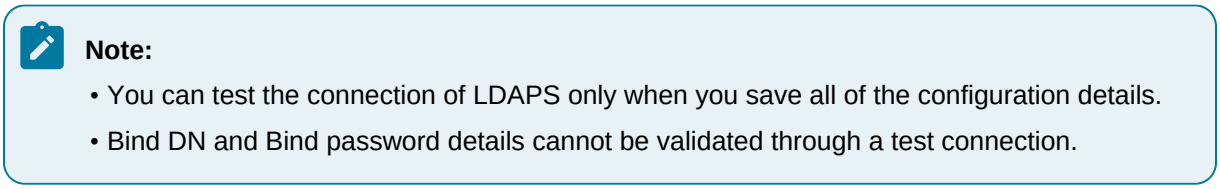
To configure the settings for LDAP or LDAPS authentication, complete the following steps:

1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config** option.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click on Configure LDAP and configure LDAP form appears in a popup.



3. In the **Host** field, enter the host address of the Active Directory (AD) server.
   The port for LDAP is displayed by default. It can be modified if necessary.
4. If you want to configure LDAPS, enable it by clicking the (Enabled) button. The port for LDAPS will be displayed automatically. You can modify it if necessary.
5. The **Upload certificate** field enabled only when the LDAPS is enabled, and then click the Browse button for the certificate you want to import.

6. In the **Bind DN** field, enter the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users. For example: cn=manager,dc=sample,dc=com The Bind DN user, such as Administrator, is the username associated with the Bind DN user account. The Connector creates a corresponding user account as an administrative user in Application Manager. You use the username for this account to log in to Application Manager as an administrator. In AD DS, the Bind DN entry must be located in the same branch and below the Base DN.
7. In the **Bind password** field, enter the password associated with the Bind DN user account.
8. You can enable Authorization to perform the validation on LDAP, leave it disabled if you want to perform the validation locally.
9. Click the **Test connection** button to ensure that the given host address is reachable and the port is valid for configuring either an LDAP or LDAPS. If the connection is successful, the following message is displayed: Test connection Success.



10. In the **Search base** field within the User search region, enter the name of the search base object that defines the location in the directory from which the LDAP search begins. For example: ou=APPVIEWX,dc=sample,dc=com An LDAP search has the potential to retrieve information about all objects within a specific scope that have certain characteristics.
11. In the **Search filter** field, enter the filters you want to use to select the entries to be returned for a search operation. These are most commonly used with the LDAP search command-line utility. For example: uid={0} The difference between uid and sAMAccountName is that uid should be unique throughout the directory name space, while sAMAccountName is only guaranteed unique within the domain. If the AD tree has several domains, there is no guarantee of uniqueness across domains.
12. In the **User return attribute** field, enter any special user attributes, such as displayID, that you want to synchronize between the local and global catalogs. Attributes associated with this type of entry can be specified, such as using the common name (CN) attribute to search for people with a specific common name.
13. Click the **Test query** button.
14. On the Test query input screen that appears,enter the following to perform the search query validation:
    - In the Test username field, enter any username available in the LDAP or LDAPS server that you are trying to configure.
    - In the **Test password** field, enter the password associated with the username.

- Click **Proceed** to check if it is a valid user.

> **Note:** You are allowed to check the query response for User search and Group search only when the connection is valid.

15. The next three fields on the tab, Group search base, Group search filter, and Group return attribute, are related to those in steps 6–8 above. The difference is that they search and fetch group membership details and also provide authorization for the group the user is associated with.
    For example, enter ou=secgrp,dc=sample,dc=com for the Group search base, 'member=*' for the Group search filter, and cn for the Group return attribute.

> **Note:**
> The search filter 'member=*' matches any entry in the directory. Since every entry is a member, and the member attribute is always indexed, this is a useful search filter to return every entry.

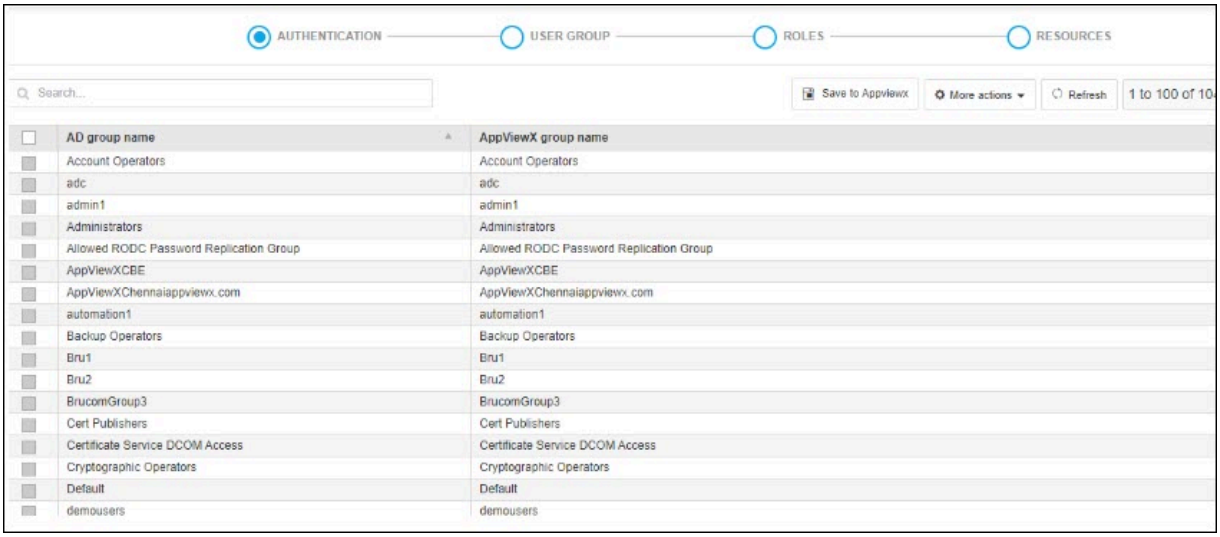
16. Click the **Test query** button to check if it is a valid group.
17. In the **Authorization map** field, select how you want to map the return attribute:
    - Select the **User group** radio button to map the attribute to the user group.
    - Select the **Role** radio button to map the attribute to the role.
18. Click **Save** to save the LDAP or LDAPS configuration and have it added to the list at the LDAP Inventory table.

> **Note:**
> - To delete an existing configuration in the LDAP inventory table, select the required LDAP configuration using the **Select** checkbox nearby the respective configuration → click on **More Actions** and from the drop down options click the (Delete) button for the configuration.
> - To update an existing configuration in the LDAP inventory table, click on the Host Hyperlink, modify LDAP popup appears → update the required details → then click on **Update**.

19. In the table, click **Fetch user groups** which exist as second column to view the user groups available in the AD and create or map them with the existing user groups in AppViewX.
20. In the popup screen that appears, fetch user groups specific to a user option selected by default, then type the username of an AD user.
21. To pull specific user groups by user group name from AD into AppViewX based on specific patterns/ keywords/code, select Fetch User groups option, then type the user group name in AD.

- Either an exact group name or using a wild character search(asterisk (*) - Matches any number of characters. You can use * anywhere in a character string)
- Example: To search User groups names containing ‘admin’, type user group name as ‘admin*’ in the search text box. All the user groups names containing admin in AD will be retrieved.

22. Click **Fetch**. A table containing the AD group names and their corresponding AppViewX user group names is displayed.



23. Select the AD user group(s) that must be created with the same name in AppViewX and click the **Save to AppViewX** button.
24. You can also select the AD user group(s) to be mapped with the existing AppViewX user group and click the **More Actions** → **Create Map** option in the dropdown → select the required existing AppViewX user group to be mapped from the Mapping user group popup → then click on **Save**. Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will be reflecting AD group names table.
25. You can also export the specific fetched AD groups by selecting specific AD groups → click on **More Options** → **Export**→ From the export user groups popup, select **Selected group(s)** option and click **Yes** → selected user group(s) should be automatically exported in `.csv` format.
26. You can also export all the fetched AD groups by clicking on **More Options** → **Export**→ from the export user groups popup, select **All user group(s)** option and click **Yes** → All user group(s) should be automatically exported in `.csv` format.

TACACS

The AppViewX system allows you to add more than one Terminal Access Controller Access-Control System (TACACS) server for authentication.

To configure the settings for TACACS authentication,

1. Navigate to **Settings** > **General** > **Authentication** > **Quick Config**.
2. Click the **TACACS sub-tab**, and then click on **Configure TACACS** button.
3. Enter the name of the TACACS authentication server in the configuration popup.
4. Enter the IP address for the TACACS authentication server.
5. Enter the port for the TACACS authentication server.
6. Click the **Test connection** button to ensure that the given host address is reachable and the port is valid for configuring TACACS.
7. Enter the secret key text string that is shared between the TACACS server and AppViewX.
8. Enter the kind of network service that will be used: for example, PPP.
9. Enter the kind of protocol that will be used. In most cases, this is IP.
10. Enter the role key, which is the return attribute from the TACACS server: for example, Role.
11. Click **Add** to save the TACACS configuration in the AppViewX system and have it added to the list at the TACACS Inventory table.

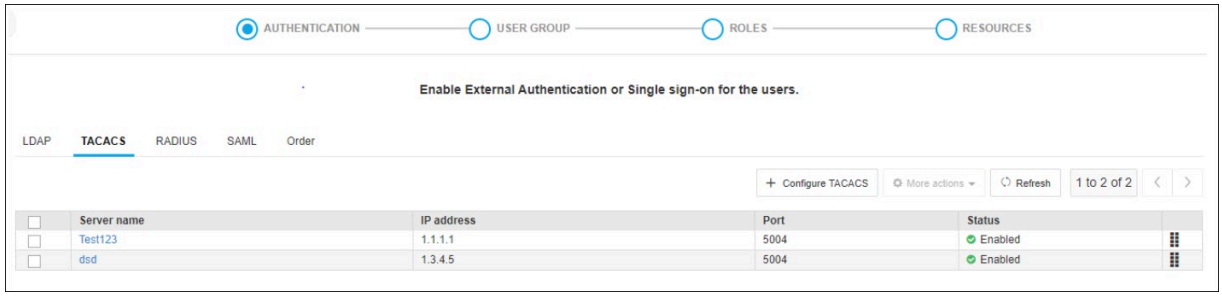
Note:

- To delete an existing configuration in the TACACS inventory table,
  - Select the required TACACS configuration using the Select checkbox nearby the respective configuration.
  - Click on **More Actions**.
  - Click the (Delete) button from the drop down option.
- To update an existing configuration in the TACACS inventory table,
  - Click on the **Server Name Hyperlink**.
  - Modify TACACS popup appears.
  - Update the required details.
  - Click on **Update**.

12. To disable a server configured,
    - Select the required TACACS configuration.
    - Click on **More Options**.
    - Select the **Disable** option from the dropdown to disable a configuration, which is currently in enabled status.
13. To enable a server configured,

- Select the required TACACS configuration.
- Click on **More Options**.
- Select the **Enable** option from the dropdown to enable a configuration which is currently in disabled status.

14. (Optional) Repeat steps 2 through 11 to add more TACACS servers to the system.
15. (Optional) In the servers inventory table, click and hold a server name and drag it up or down to change the order of TACACS servers in use in the system.
    Order will be automatically saved.



Chapter 7: Control Center

Overview

Control center module is a centralized object repository which allows the user to manage and monitor the objects. To manage and monitor the objects AppViewX provides some basic action in right click of object in control center. The objects will be categorized into three types based on which the right click actions may vary.

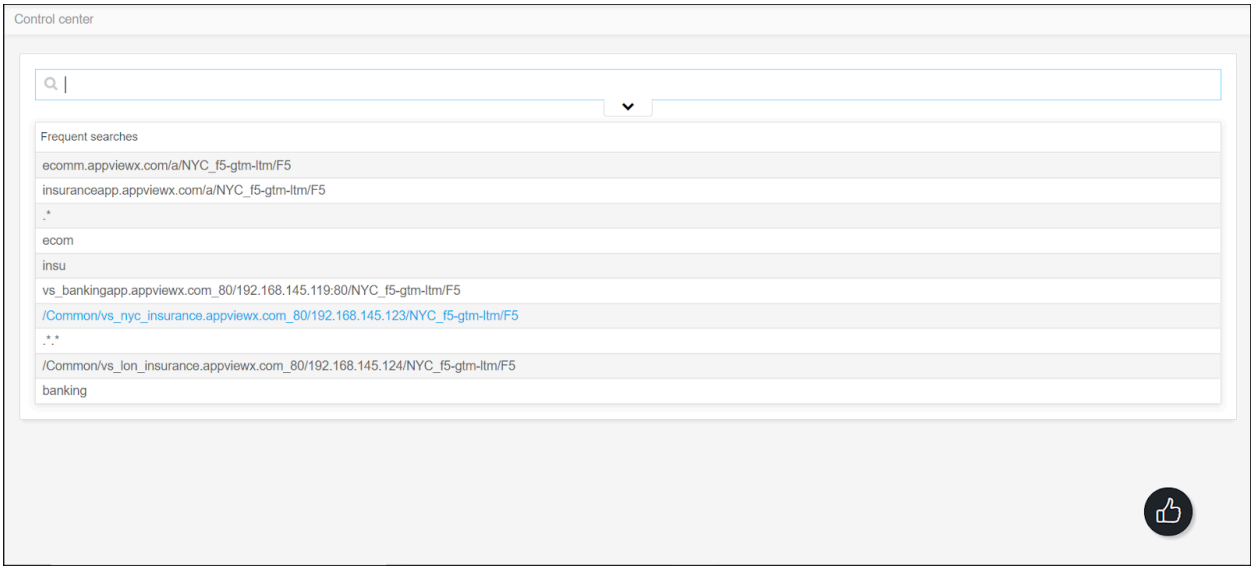
- **Primary objects** - Objects that are used in load balancing. These objects have access permission at individual level. For example in F5 objects like wide ip, pool, pool member, server are considered as primary objects.
- **Orphan objects** - Objects without parents will be considered as orphan objects. For orphan objects AppViewX allows the user to provide access in global level not at individual level. For example, an F5 pool that is not associated with wide ip will be considered an orphan pool.
- **Secondary objects** - Objects that are associated with primary objects but which do not directly participate in load balancing are called secondary objects. AppViewX provides global level access permissions for secondary objects. For example monitors, profiles, etc., Where monitors are used to monitor the health of the servers.

Before you begin

- Devices that the user wants to control should be added to AppviewX.
- Users must have the ACF permissions to access the Control Center. Users should also have the object level access (ACL) in the resources.
- To perform actions on objects users should have proper ACF permission and ACL permission.

Search

The App Search module displays a centralized object repository from the Control Center that allows you to search for and then monitor and manage all the entities, configurations, or objects of the ADC devices. Control Center provides a holistic NOC overview for app teams and network teams to quickly search and monitor application services based on RBAC in a visual intuitive topology view.



In App Search module, the Control Center acts as a search engine inside the AppViewX to search and monitor any Application in your infrastructure. From the app search, any application-related details can be searched/found the complete infrastructure details and services supporting the application. The Control Center within the App Search module also provides better insights into the configuration, state, and performance of the application and helps to troubleshoot application outages more effectively.

To use the Control Center within the App Search module, the following prerequisites must be met:

- Each device you want to control must have been a managed entity in AppViewX.
- A role and resource must have been assigned with the appropriate device/object level that you want to control. However, for the orphan and secondary objects, global access must have been provided.

Search Using Free Text Entries

This is the most common type of search. You can enter text in the search field and press Enter on your keyboard. The following search features and functionalities are supported:

- Case insensitive keyword and string matching. For example, the search result for F5 would be **f5_86.appviewx.com**.
- Exact match search strings through the use of double quotation marks around search terms. For example, "**gs-f5-pe21.lab.appviewx.net**".
- Entering only the application name in the search field is enough to find all the hierarchical details related to it.
- Boolean AND and OR operators:
  - **AND Operator** - search results contain both terms that existed in the search query. For example, **gs-f5-pe21.lab.appviewx.net AND default**.
  - **OR Operator** - search results contain one or both terms that existed in the search query. For example, **gs-f5-pe21.lab.appviewx.net OR default**.
  - **AND** and **OR** - When a Boolean AND operator and an OR operator exist in the same search string, the AND operator is executed first by default. For example, **gs-f5-pe21.lab.appviewx.net AND gs-f5-pe51.lab.appviewx.net OR default.**

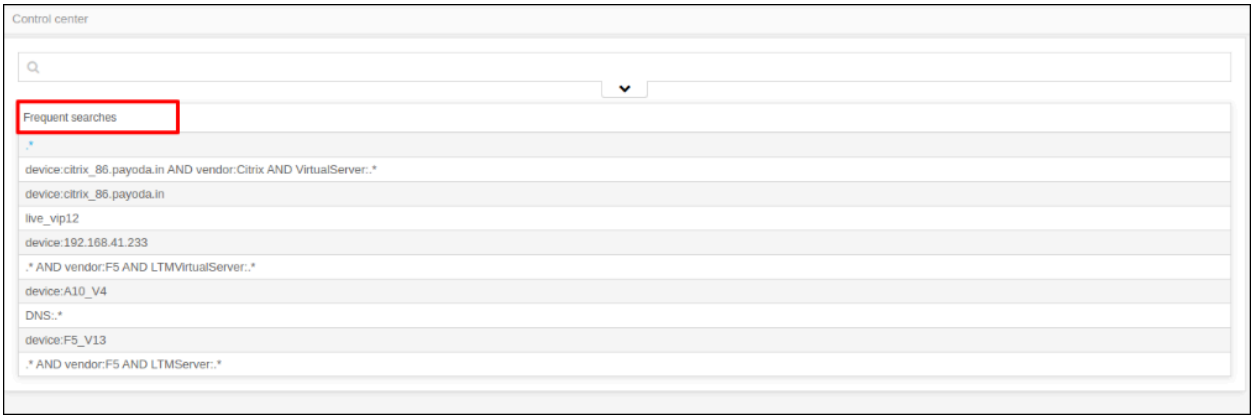
If parentheses appear in a Boolean query, the query components within the parentheses are executed first, followed by the query components outside the parentheses. For example, **(gs-f5-pe21.lab.appviewx.net AND default) OR 3.4.5.6**.

For example, typing only the application name in the search bar is enough to find all the hierarchical details related to it:

Search Using Frequent Search Links

The App Search screen displays a list of frequent searches immediately below the search field. Click any of the items in the Frequent searches list to search the AppViewX platform for that word, phrase, or character set.

In the ADC search results screen, click the vertical ellipse button next to the search bar and select **Frequent Searches** to view a list of frequent searches.



Search Using Predefined Search Keys

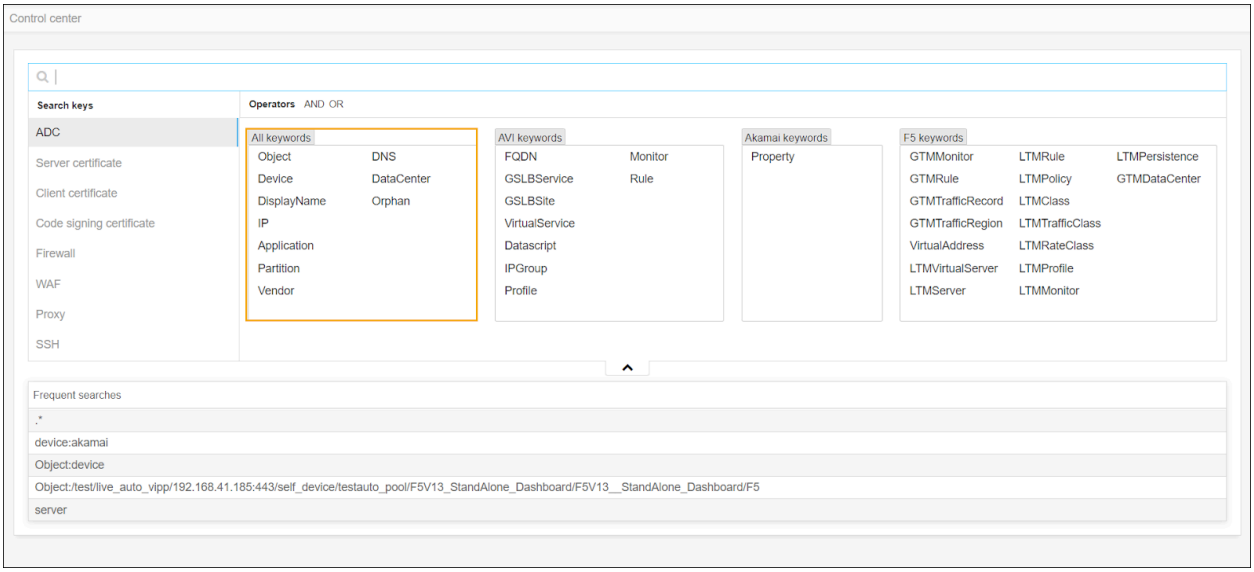
AppViewX provides a set of predefined keys specific to each ADC vendor to help the search operation. The types of predefined keywords are:

- All keywords
- Vendor-specific keywords
- Logical operator with keywords

The predefined search keywords can be used to create highly targeted search queries. To create a search query, see create a search query.

All Keywords

These keywords are generic to all ADC vendors and help searching objects irrespective of vendors.



Sample Search Keywords

Common Keywords	Description
Object:	Search for objects using the name.
Device:	Search for objects from a particular device managed in the ADC inventory.
Displayname:	Search for objects using the Displayname. Displayname represents the naming format of your objects that needs to be followed throughout the application. Refer <displayname section>
IP:	Search for objects using the IP address. Eg: Objects like Virtual Servers, Pool members that belong to a particular IP can be searched.
Application:	Search for objects associated with an Application name.

Common Keywords	Description
	AppViewX tags all the hierarchical objects of an Application using the WideIP name as a tag during every config fetch.
Partition:	Search for objects from a device partition or tenant or context.
Vendor:	Search for objects from a particular vendor (F5, AVI, etc.,)
DNS:	Search for objects using their DNS name. AppViewX performs a scheduled (twice a day) reverse lookup for the objects that contain an IP address in it and persists the DNS name of the objects.
Datacenter:	Search for objects from a particular Datacenter. Datacenter name information should have been provided at the time of device addition.
Orphan:	Search for objects that do not have Parent association. Objects like GTM/LTM pools that are not associated with WideIP/Virtual Server will be considered as Orphans.

Logical Operator with Keywords

The common keywords and Vendor specific keywords can be combined with any Logical operator.

Sample Keywords

Keywords	Description
virtual server:* AND device: F5_v11	The list of virtual servers available in the F5_v11 device.
device: F5_v11 AND virtual server:* AND IP:192.168.96.101	The list of virtual servers in the F5_v11 device that uses the IP address 192.168.96.101 is identified.

Create a Search Query

To create a search query:

1. On the **Search** screen, click the  (**Expand**) tab at the bottom of the search field.
2. The field expands to display a list of search keys available for the ADC.
3. For each metadata type, you add to the search query, enter a value or partial value to search for. If you enter no text after the search key, the search engine automatically searches for "all values."

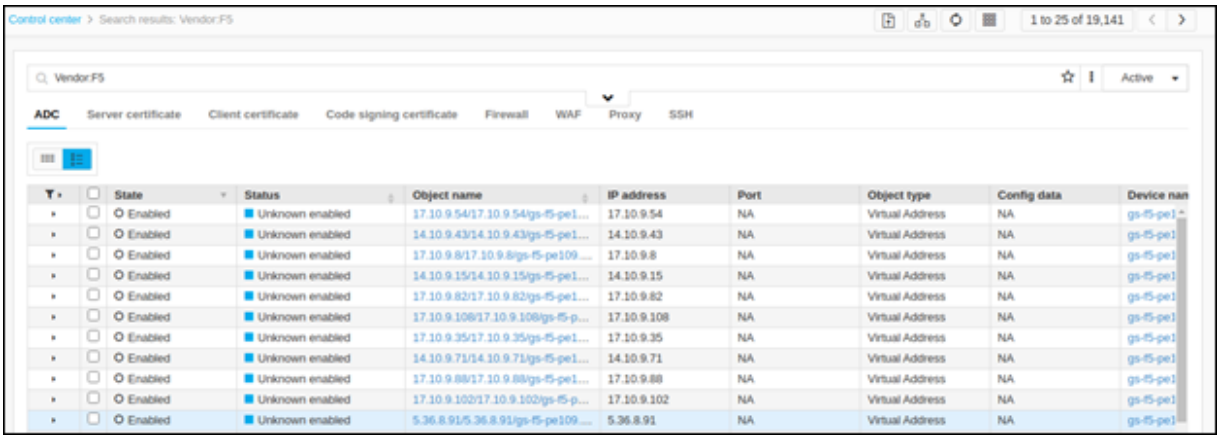
4. (Optional) Click the AND and OR operators at the top of the Search keys field to create Boolean searches.
5. When you are finished creating the search query, click inside the search field, then click Enter on your keyboard to run the search.

View the Object Details

1. The object details are represented in the form of a tabular with additional information as follows:

Column name	Description	Default?
State	State of the objects.	Yes
Status	Status of the objects.	Yes
Object name	Based on the display name configured.	Yes (mandatory)
IP address	The IP address of the objects.	Yes
Port	Port of the IP address.	Yes
Object type	Type of object.	Yes
Config data	Configuration of the objects is displayed in a Pop upon clicking the link.	Yes
Device name	The device name of the object. On clicking, the user is redirected to the device addition page.	Yes
Vendor	Vendor of the object.	Yes
Device IP/FQDN	IP or FQDN of the device. The user is redirected to the device login on clicking.	No
Connection count	Display the live connection count of the objects if applicable.	No
Partition	Partition/tenant/context of the objects if applicable	No
DNS name	DNS resolution of the objects if applicable.	No

2. In the search results field, hover your cursor over the result whose basic details you want to view.



Filter the Objects

To filter the objects in the Infrastructure view,

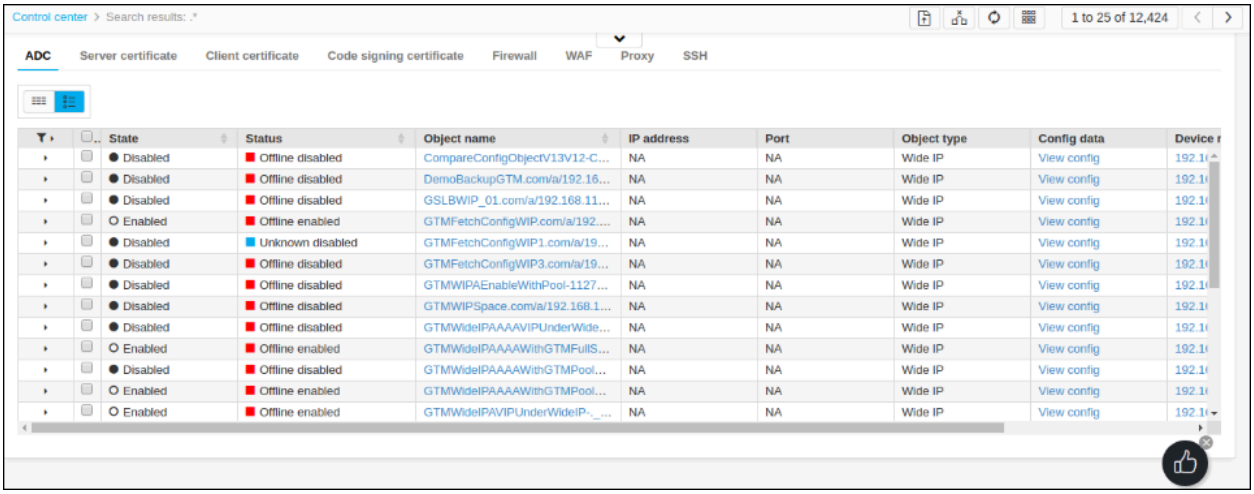
1. Run a search.
2. Click the filter icon located at the first cell of the table.
3. The filter options are enabled in the header of the table.
4. Select and/or enter the criteria to filter the objects.
   The objects that match the filter criteria are displayed.

Note:

- To remove the filter option, click again the filter icon.
- To reset the filter criteria that have been applied, select and/or remove the text that has been applied for filtering the objects.

Infrastructure View

Only the ADC objects corresponding to your search criteria are displayed and not its hierarchy (such as a parent, child 1, and child 2). By clicking the  (**Infrastructure view**) button to switch from the Application view.



Filter the Objects

To filter the objects in the Infrastructure view,

1. Run a search.
2. Click the filter icon located at the first cell of the table.
3. The filter options are enabled in the header of the table.
4. Select and/or enter the criteria to filter the objects.

   The objects that match the filter criteria are displayed.

Note:

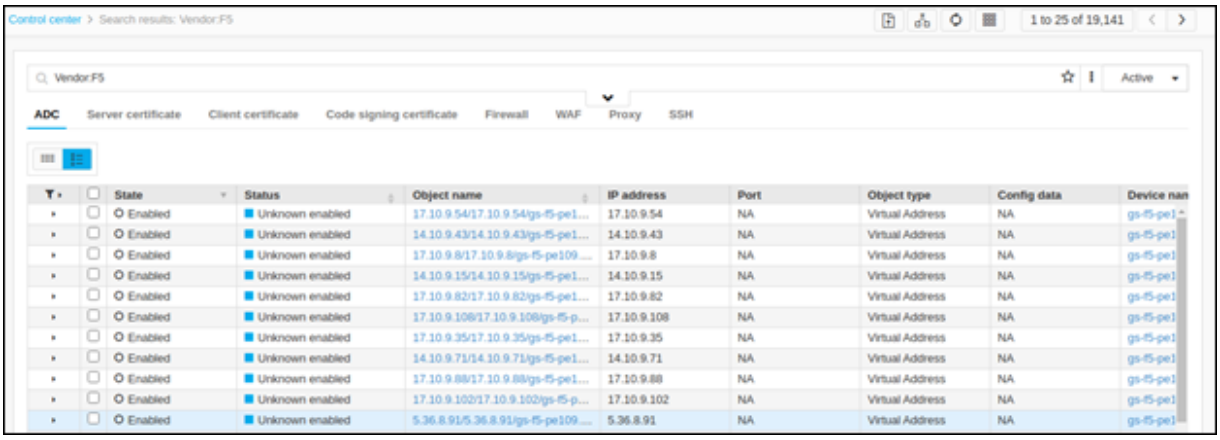
- To remove the filter option, click again the filter icon.
- To reset the filter criteria that have been applied, select and/or remove the text that has been applied for filtering the objects.

View the Object Details

1. The object details are represented in the form of a tabular with additional information as follows:

Column name	Description	Default?
State	State of the objects.	Yes
Status	Status of the objects.	Yes
Object name	Based on the display name configured.	Yes (mandatory)
IP address	The IP address of the objects.	Yes
Port	Port of the IP address.	Yes
Object type	Type of object.	Yes
Config data	Configuration of the objects is displayed in a Pop upon clicking the link.	Yes
Device name	The device name of the object. On clicking, the user is redirected to the device addition page.	Yes
Vendor	Vendor of the object.	Yes
Device IP/FQDN	IP or FQDN of the device. The user is redirected to the device login on clicking.	No
Connection count	Display the live connection count of the objects if applicable.	No
Partition	Partition/tenant/context of the objects if applicable	No
DNS name	DNS resolution of the objects if applicable.	No

2. In the search results field, hover your cursor over the result whose basic details you want to view.



- Filter the Objects
- Infrastructure View

View Additional Details of Search Results

There are two ways to view additional details about search results and the method varies depending on the type of object you are viewing:

- **Topology View**: Clicking the object takes you to topological screens that provide much more information about the corresponding object than is displayed on the search results screen.
- **ADC Topology Actions**: ADC primary and secondary object search results can be right-clicked to view the list of actions available for them.

- Topology View

Topology View

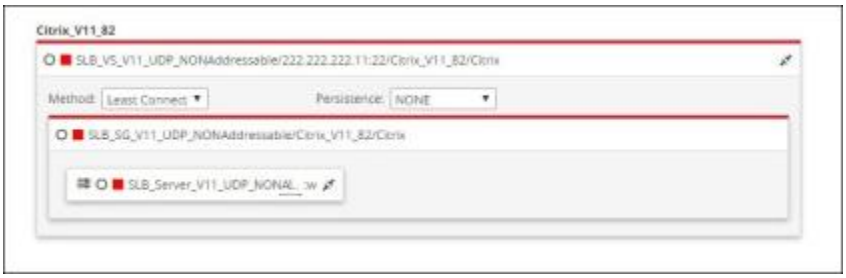
When you click a search result for a primary ADC object either from the **Application** or **Infrastructure** view, a topology view opens, providing a detailed, hierarchical map of the structure of the ADC. The following are the sample ADC topologies within the Control Center.

For example, read the topology view: GTM > LTM > Pool > Pool mem...

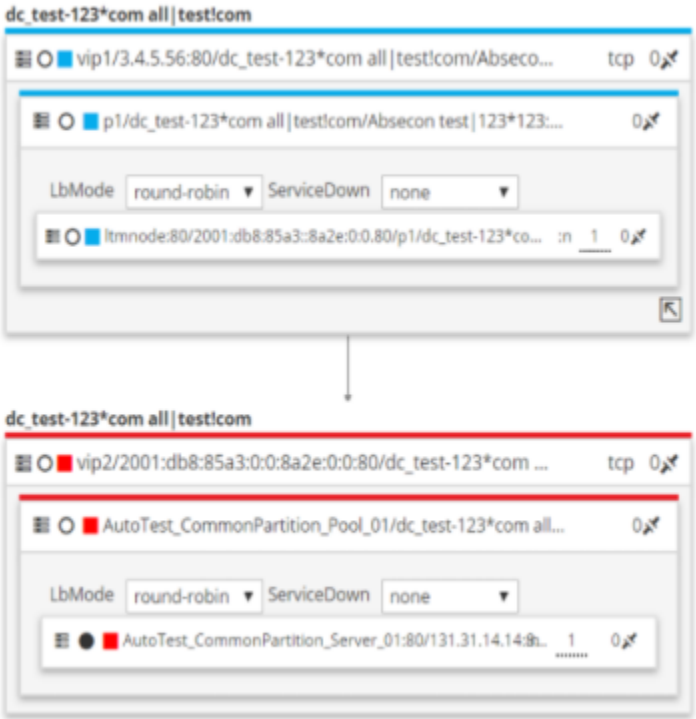
- Server Load Balancing (SLB) Virtual Server Topology
- Virtual Server IP (VIP) under VIP Topology
- Virtual Server (VIP) under Wide IP Topology

- Virtual Server (VIP)/SLB Topology
- Wide IP/GSLB Topology

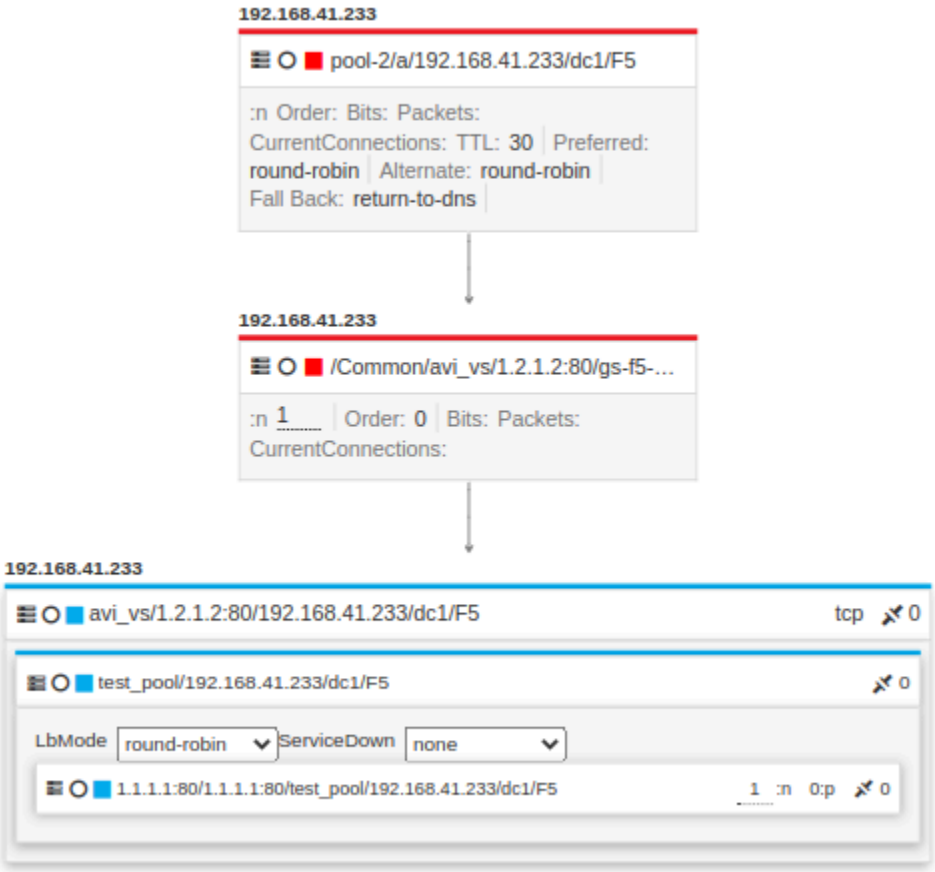
Server Load Balancing (SLB) Virtual Server Topology



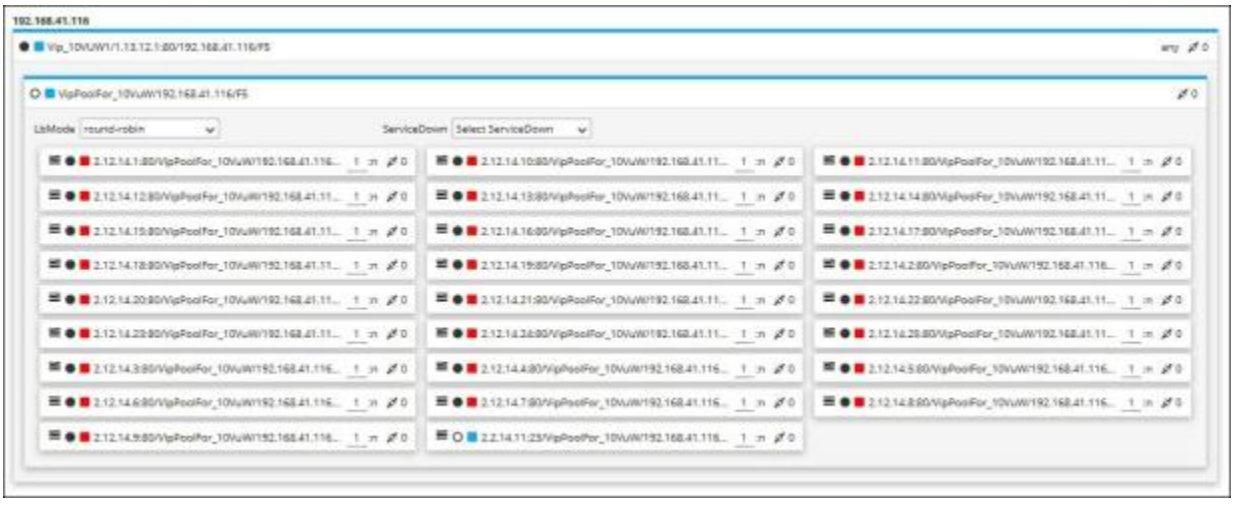
Virtual Server IP (VIP) under VIP Topology



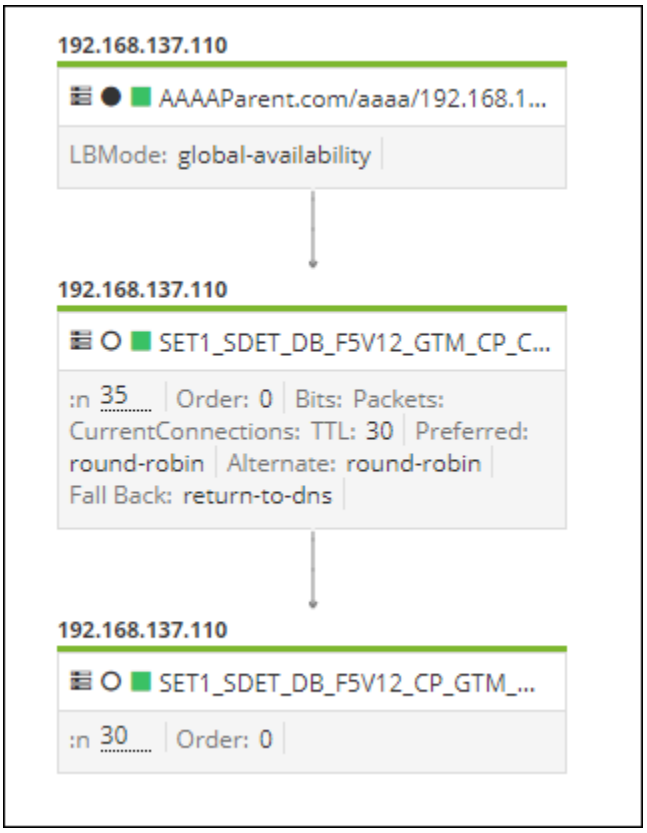
Virtual Server (VIP) under Wide IP Topology



Virtual Server (VIP)/SLB Topology



Wide IP/GSLB Topology



Bookmarks

AppViewX allows the user to bookmark the frequently used search items.

- Create a Bookmark
- Delete Bookmark

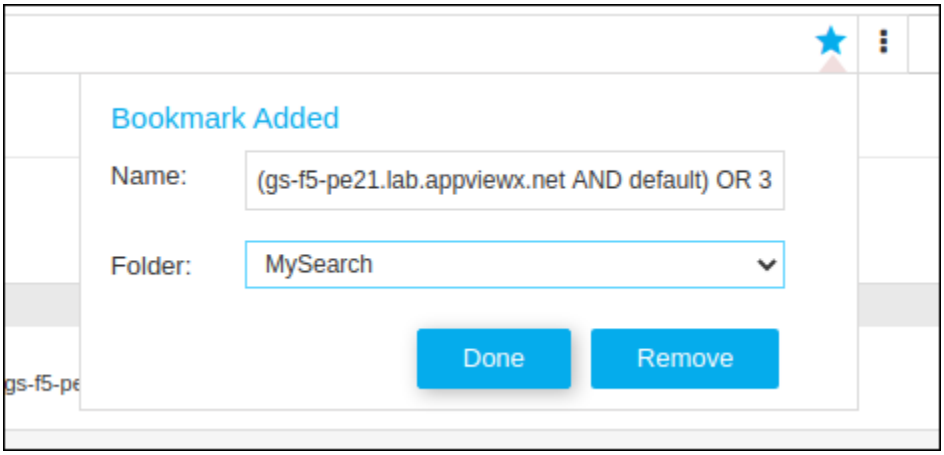
Create a Bookmark

If any search strings or search queries are repeatedly used, it can be bookmarked for future access.

To create a bookmark for the ADC frequent search items,

1. Click the **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **App Search**.
   The Control Center search screen appears.
2. Run a search.

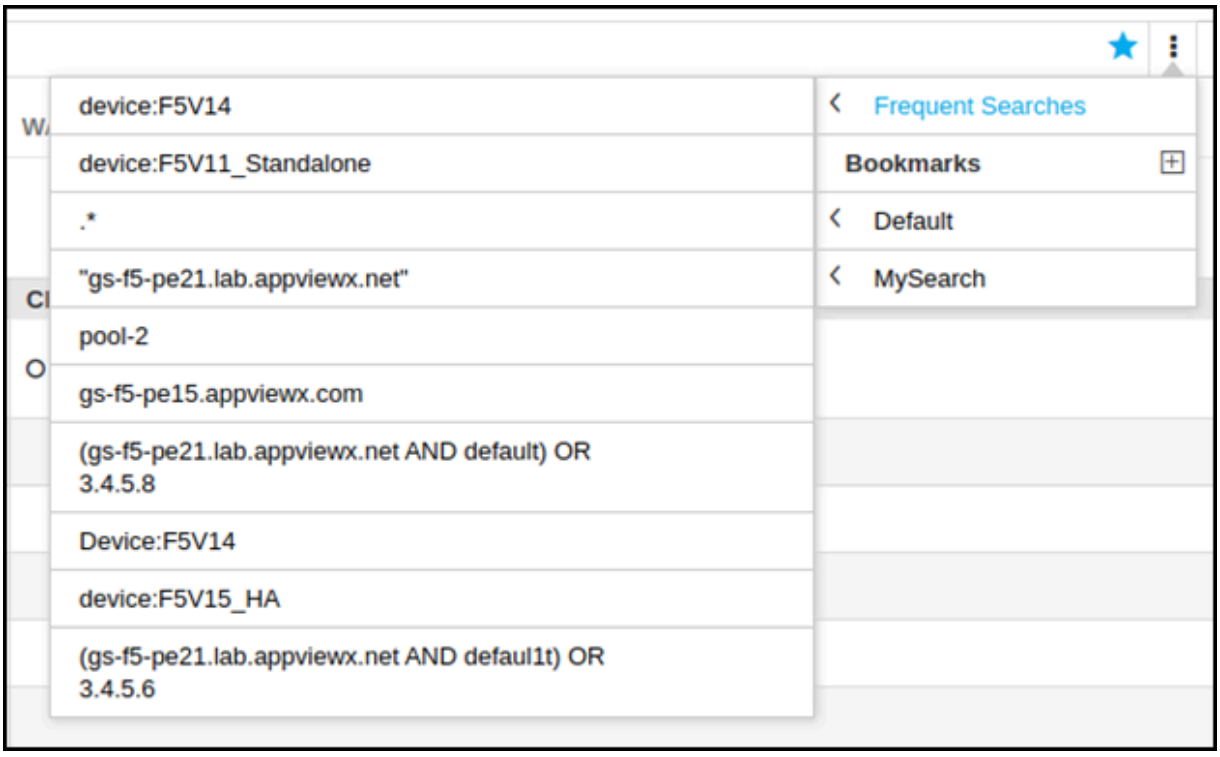
3. On the search results screen, click the button next to the search bar.
4. Click the button to create a bookmark folder.
5. Click the button on the search bar. A pop-up message will be displayed at the top of the screen, **Bookmark(s) created successfully**.
6. On the **Bookmark Added** pop-up screen, enter a name for the bookmark to help the users identify it.



7. Select the folder to which you want to add this bookmark from the dropdown list and click **Done**.

> **Note:** If you want to delete the bookmark, click the Remove button. A pop-up message will be displayed at the top of the screen, Bookmark(s) deleted successfully.

Queries that are frequently used are added to the frequent searches by default and the top 10 queries can be accessed in a single click as below:



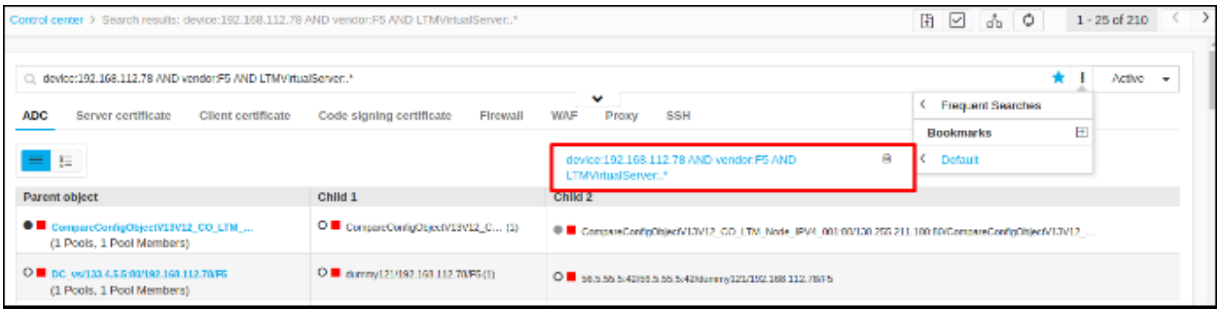
Delete Bookmark

Follow the below steps to delete a bookmark.

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Control Center**.
3. Run a search.
4. In the grid / infrastructure view click on **More Options** button(3 vertical dots) next to the search bar.

5. Mouse hover the folder name under the bookmarks menu.

All the bookmarks under the folder will be displayed.



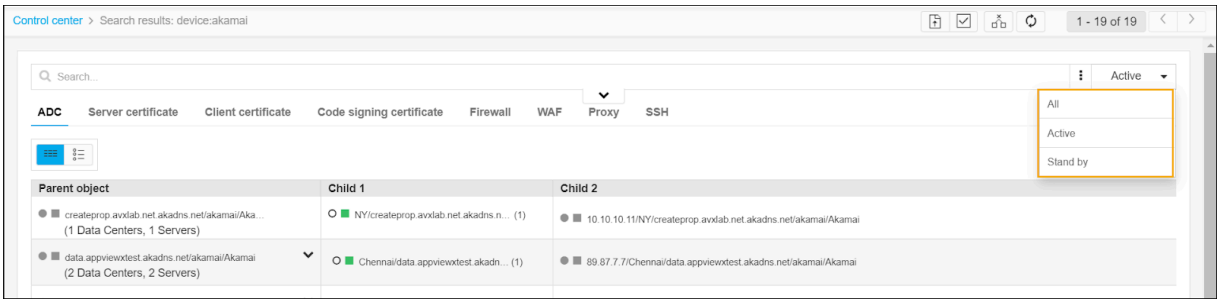
6. Mouse hover on the bookmark name and the delete button will be displayed.

7. Click **Delete**.

Filter ADC Search Results

To filter ADC search results within the Control Center:

1. Run a search.
2. On the search results screen, click the **Active** drop-down option.



3. Select one of the three filter options in the dropdown list that appears:
   - **All** - View all search results, regardless of status.
   - **Active** - View search results for objects with a status of Active.
   - **Stand by** - View search results for objects with a status of Standby.
4. The screen then refreshes and filters the results on both the Application view and Infrastructure view based on the filter you selected.

Export Search Results

When you search for the objects in the Control Center, the objects that match the search keyword are displayed in the Application view. The resulting objects can be exported. You can export the selected objects or all the resulting objects.

To export objects search results within the Control Center,

1. Run a search.

   By default, the search results are displayed in the  (**Application view**) page.
2. Click the checkboxes beside the object name to select the object details that you want to export from the grid or select all of the ADC objects by clicking the  (**Select all**) button in the Command bar.
3. All of the search results on the screen display with a blue background to indicate that they have been selected.
4. Click the  (**Export**) button in the Command bar.
   The .csv file is downloaded to your computer.
5. If you want to export the search results displayed on the infrastructure view,  (**Infrastructure view**) button to switch from the Application view search result page and do the following:

- Select the checkboxes beside the first column of the grid to select the object details that you want to export from the grid. You can select all of the objects from the search results screen by selecting the first checkbox in the grid.
- Click the  (**Export**) button in the Command bar.
- On the **Export** screen that pops up, select either the **All columns** or the **Displayed columns** radio button based on what you want to export from the grid.

  The `.csv` file is downloaded to your computer.

Orphan Objects

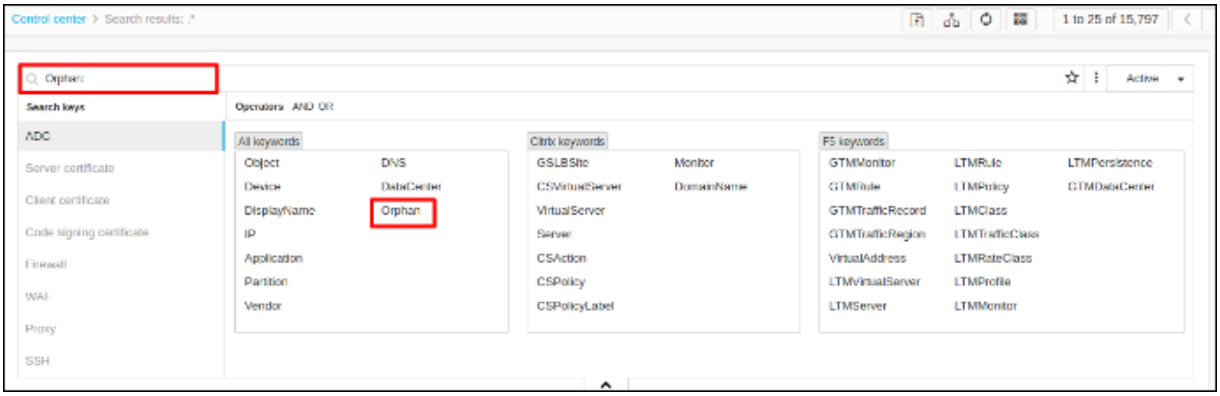
Objects without parents will be considered as orphan objects. For example, an F5 pool that is not associated with wide ip will be considered an orphan pool.

There are two ways to view the orphan objects in the Control Center.

- Using Orphan Keyword
- Using Orphan Objects Button

Using Orphan Keyword

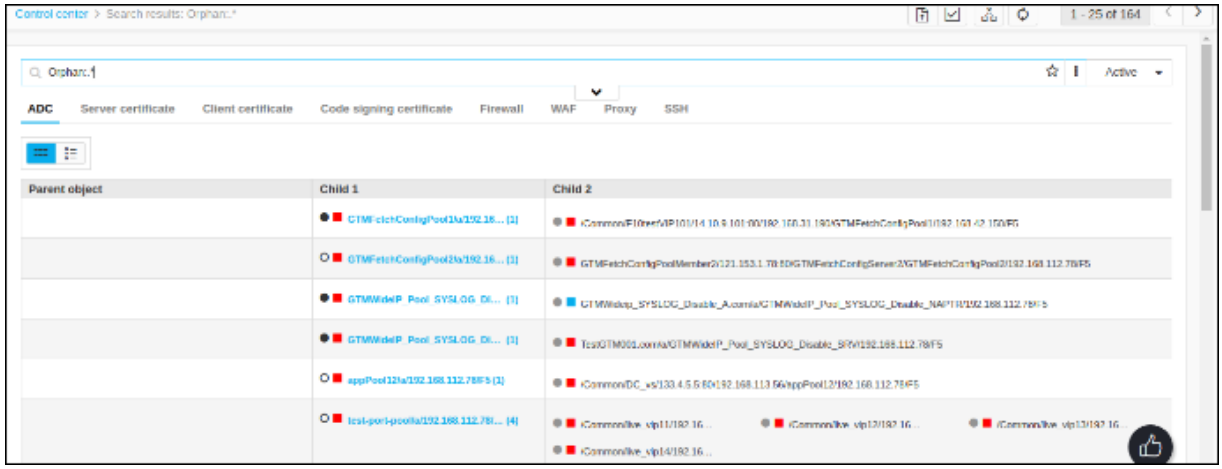
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Control Center**.
3. Expand the keywords tab.
4. Click on **Orphan** keyword from the all keywords section and click enter.



Using Orphan Objects Button

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Control Center**.
3. Run a search.
4. From the grid / infrastructure view click on the **Orphan Objects** button.

5. In the grid view, the parent column will always be empty for the orphan object.



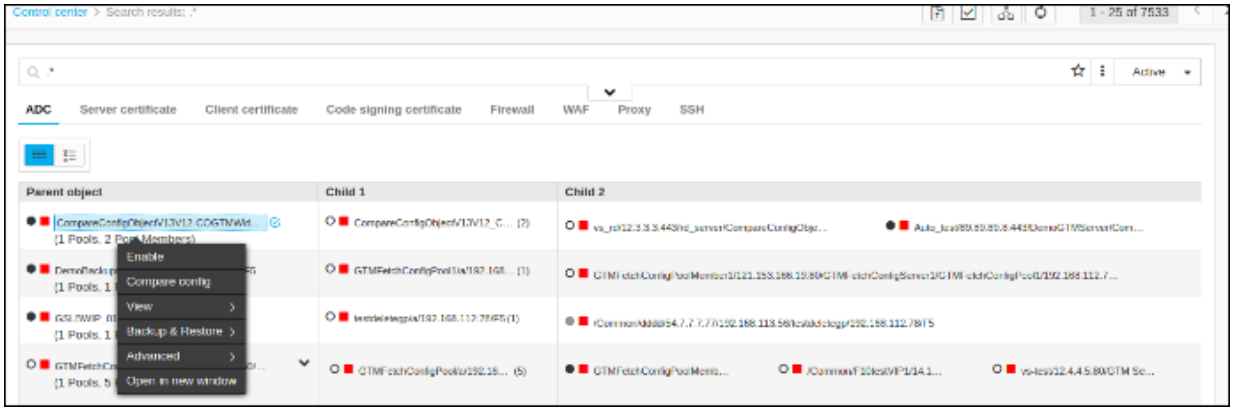
Right click actions

AppViewX provides some right click actions for objects in all the views. Users can do right click action on individual / multiple objects. The actions that appear on the list may vary depending on the object type and the vendor.

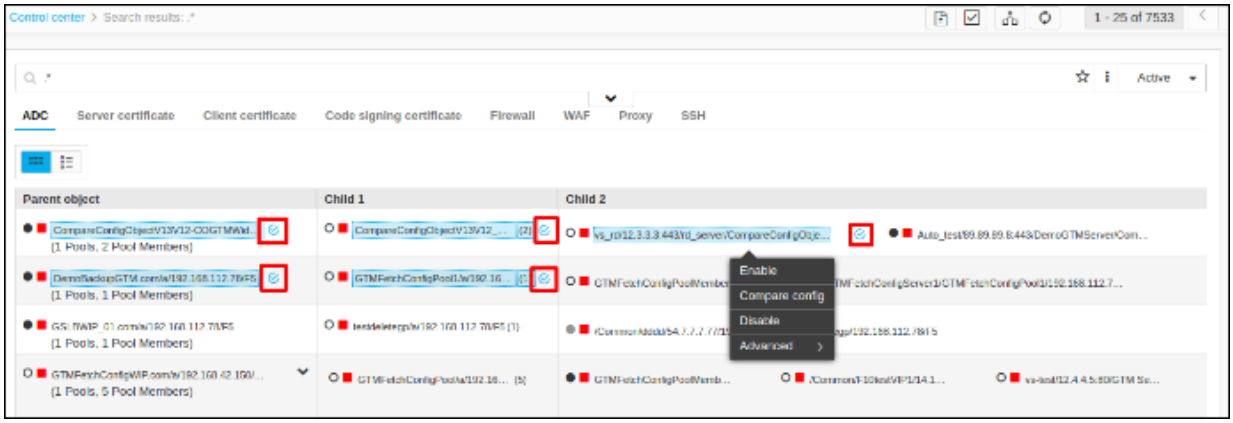
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Control Center**.
3. Run a search.

Executing From Application View

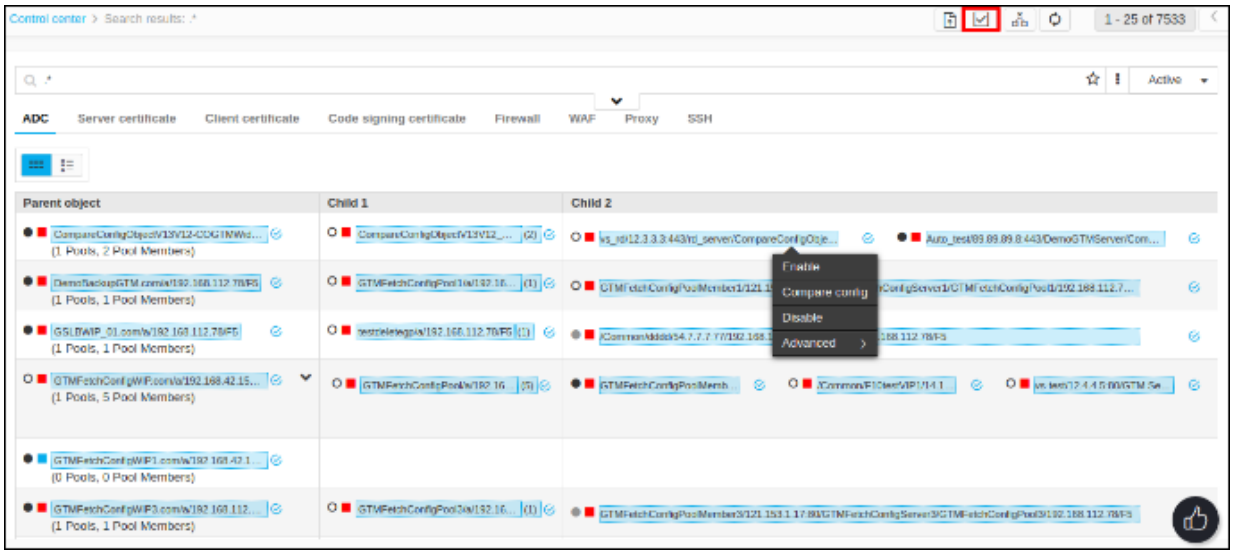
- Users can do right click actions on individual object level in grid view. To do an action on an individual object right click on the object.



- Users can do right click actions on multiple objects level by selecting the objects using the Select button near the object. After selecting the objects do a right click. When the user clicks on a particular action the actions will be applied only for the applicable actions from the selected objects.

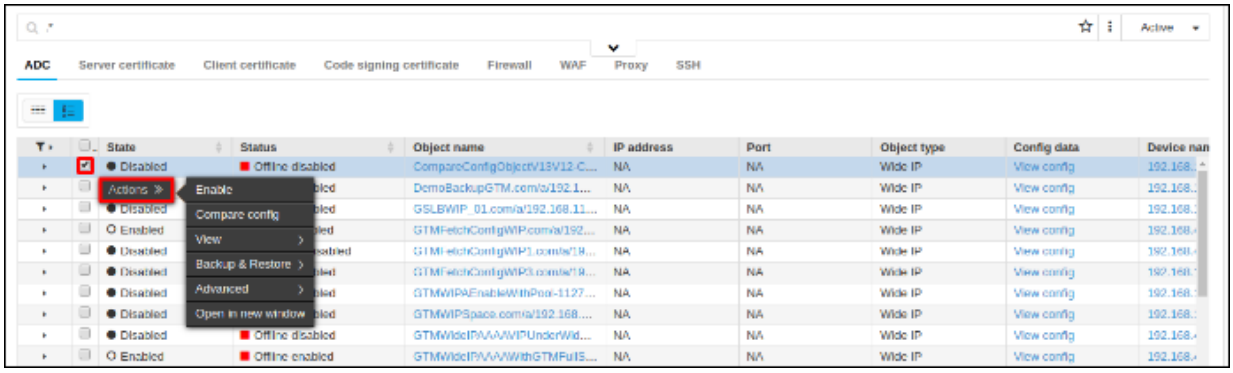


- Users can do right click actions on all the objects in the page. When the user clicks on the Select All button in the top right corner and then right click on the objects. When the user clicks on a particular action the actions will be applied only for the applicable objects from the selected objects.

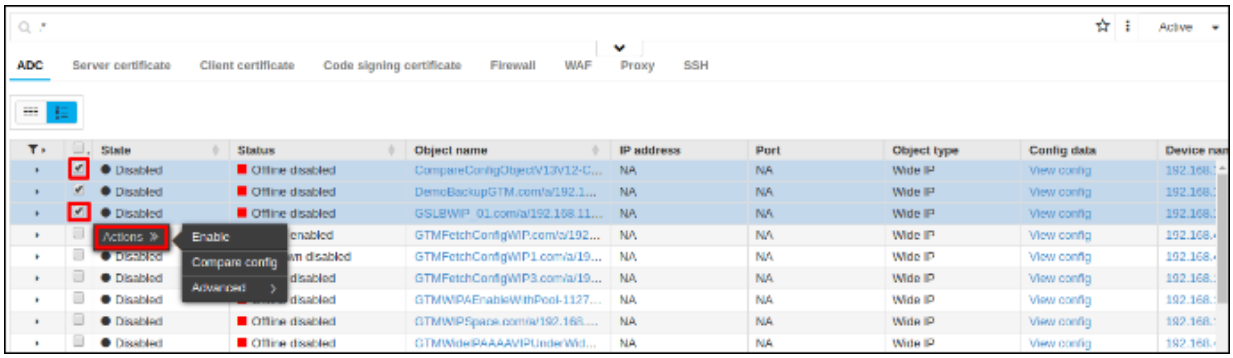


Executing From Infrastructure View

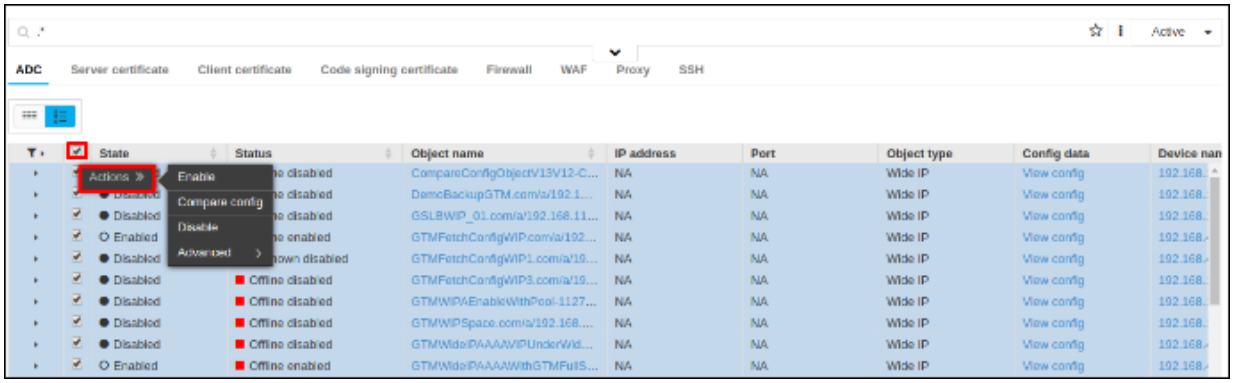
- Users can do right click actions on individual object level in grid view. To do an action on an individual object, select a single object and hover on **Actions**.



- Users can do right click actions on multiple objects level by selecting the checkboxes of the object. After selecting the objects hover on **Actions**. When the user clicks on a particular action the actions will be applied only for the applicable actions from the selected objects.

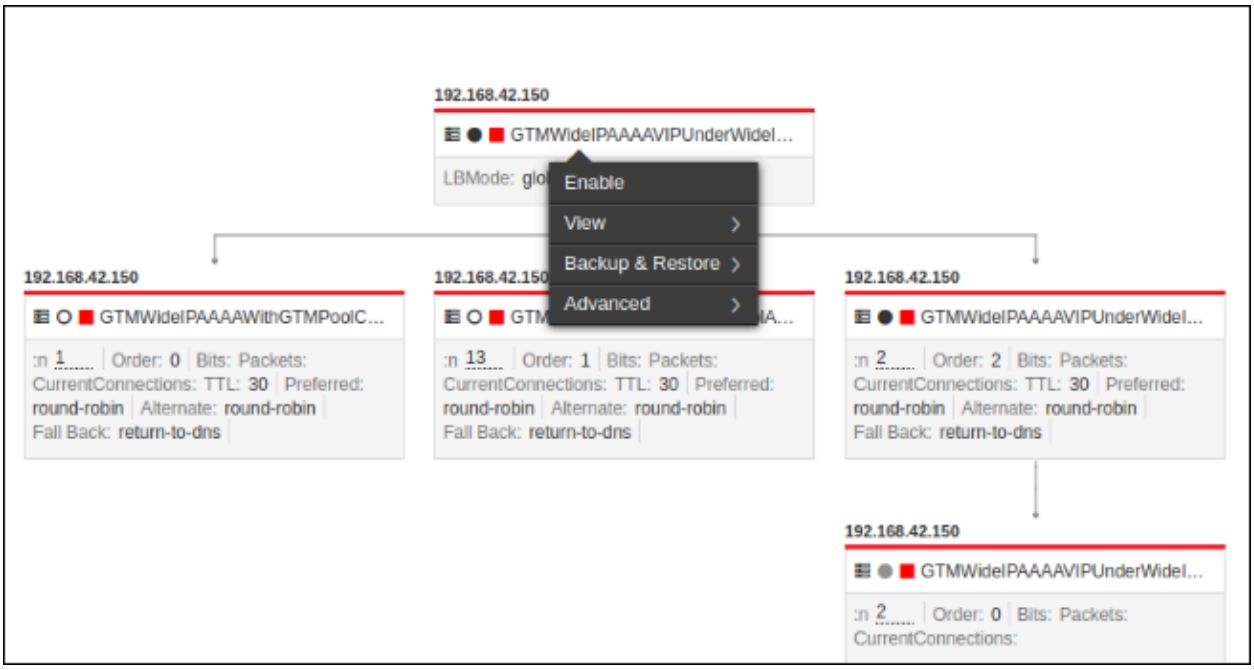


- Users can do right click actions on all the objects in the page. Users can select all the objects by selecting the **Select all** checkbox (first checkbox in the grid). When the user clicks on a particular action the actions will be applied only for the applicable objects from the selected objects.



Executing From Topology View

From topology view users can do right click actions on individual objects. To do an action on an individual object right click on the object and click the required action.



Below are the right click actions supported in AppviewX. Basically they fall under two categories.

- **Write actions** : These actions will change the configuration of the object in the device and the respective changes will get updated in AppViewX also. Whenever the user triggers the below actions user will get a **Comments box** for most of the actions, where the entered comments will be maintained in auditlog. To perform the action users should enter a valid comment in that and then click **Yes.**
  - Enable
  - Disable
  - Force down
  - FD clear active connections
  - Enable all
  - Disable All
  - Forcedown all
  - Enable persistence
  - Disable persistence
  - Restore object
  - Clear persistence
- **Read actions** : These are the view actions. This will not modify any configuration.
  - Compare config
  - View source connections
  - View persistence
  - Backup device

- View graph
- View config
- View log
- View Alerts

Actions

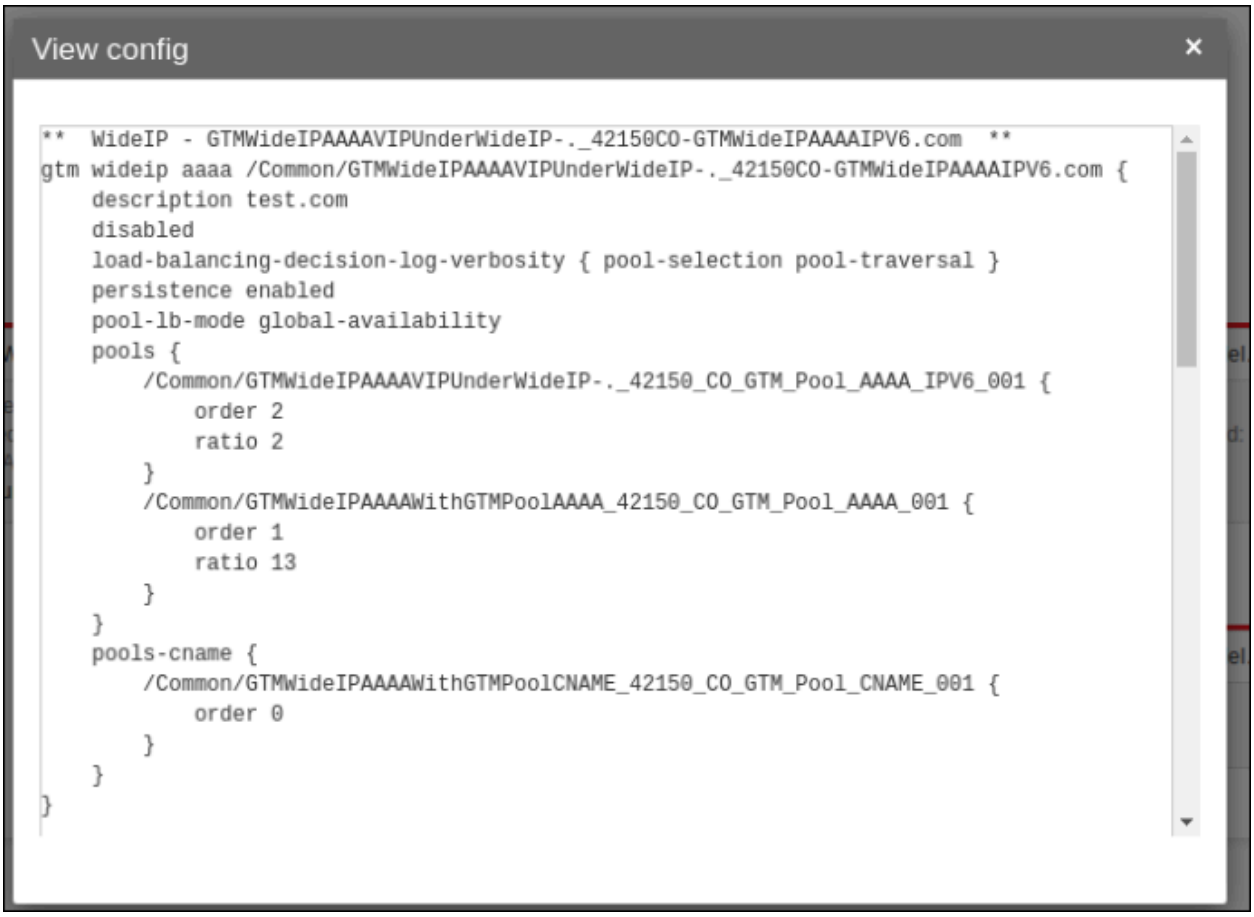
Action		Description
Enable		Enables the Object.
Disable		Disables the Object.
Force Down (Specific for F5)		Force down the object.
FD Clear Active Connections (Specific for F5)		Force down the object and terminate all the current connections.
Graceful disable (Specific for AVI)		Disable the object only when all the current active connections are closed either by server or client.
Compare Config		Compare current and /or archived configurations of objects with the same name.
View Source Connections (Specific for F5)		View the active connections for VIP and LTM Pool.
View Persistence (Specific for F5)		View the persistence for VIP and LTM Pool.
Clear source Connections (Specific for F5)		Clear the persistence for VIP and LTM Pool.
Open in New Window (Grid / Infrastructre View)		Displays the topology view of the selected object in the new window.
Backup & Restore	Backup Device	Create the backup of the device associated with the object. Backup will be available in the Default backup group.

Action		Description
	Restore Object	Restore the object configuration to a previous state.
Advanced (Specific for F5)	Enable All	Enable all the LTM pool members with the same ip port on the same device.
	Disable All	Disable all the LTM pool members with the same ip port on the same device.
	Force Down All	Force down all the LTM pool members with the same ip port on the same device.
	Enable Persistence	Enable or Disable the tracking and storing of session data, which is used to ensure that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.
	Disable Persistence	
View	View Config	View the configuration of the object and its child objects.
	View Graph	View the timeline statistics for the object.
	View Log	View the log history specific to this object.
	View Alerts	View the alerts related to this object.

- View Config
- View Graph
- View Log
- View Alert

View Config

Shows the configuration of the selected object and its child.



View Graph

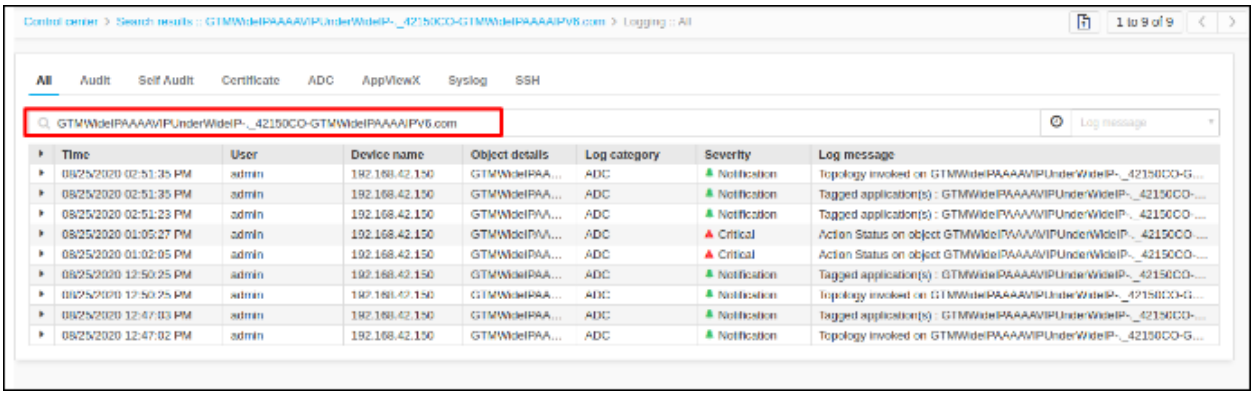
Shows the timeline statistics for the selected object. Graph will be available only if the statistics is configured in the Settings. For more details on settings refer Configuring statistics collection.

When the user clicks on the view graph pop-up will be displayed.

- **Statistics** - The entries in this list vary depending on the object. when the user selects the different stat parameters the corresponding graph will be updated.
- **Interval** - The following time intervals can be selected: **Day**, **Week**, **Month**, or **3 Months**. When the user selects different intervals the graph displayed will be updated to the selected time frame.

View Log

When the user applies the view log action on particular objects, the audit logs related to that particular object alone will be filtered and displayed.



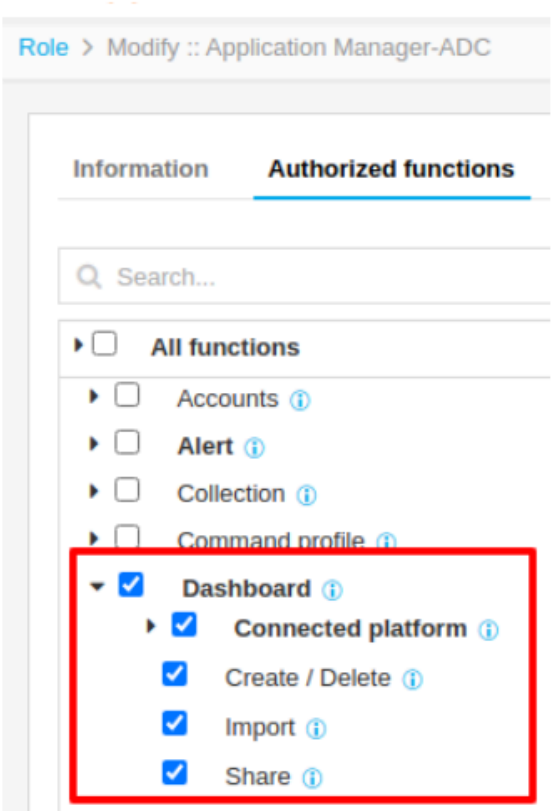
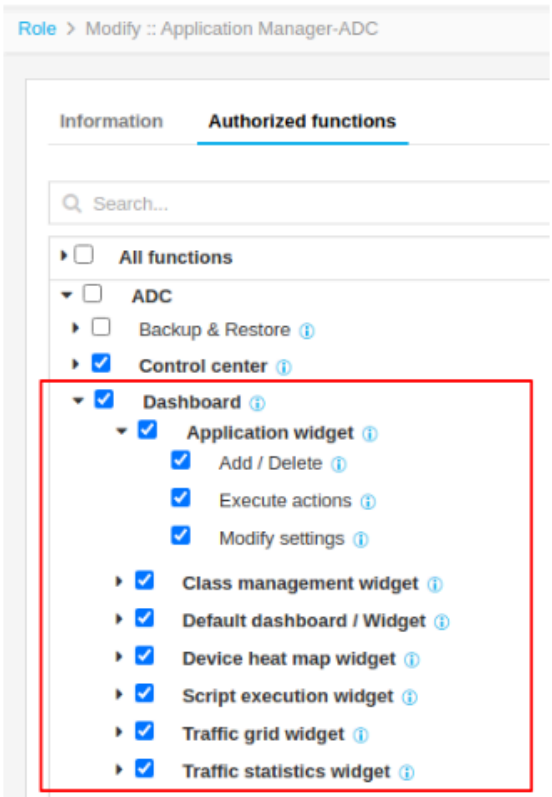
View Alert

When the user applies the view alert action on particular objects, the alerts related to that particular object alone will be filtered and displayed.

Chapter 8: Configuring Dashboard

Before you begin

• To configure dashboards and widgets, the user should have ACF permissions.

Access for Dashboard:	Access for ADC Widgets:
	

- For adding objects in the widgets, the device should be Managed in the inventory and the user should have object level access (ACL) in the resources. For performing actions on the object, RW permission should be provided.

Default Dashboard

TheDefault ADC Dashboard is pre-configured and has a default set of widgets. The widgets are Device heat map, Top 10 VIPS by Connection, Application Heatmap, Number of Objects, Top 25 Applications by Connection and Unused Objects Report.

To view the reports related to ADC,

1. Go to **Menu** > **ADC+** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.

   A pre-built ADC Dashboard appears by default.

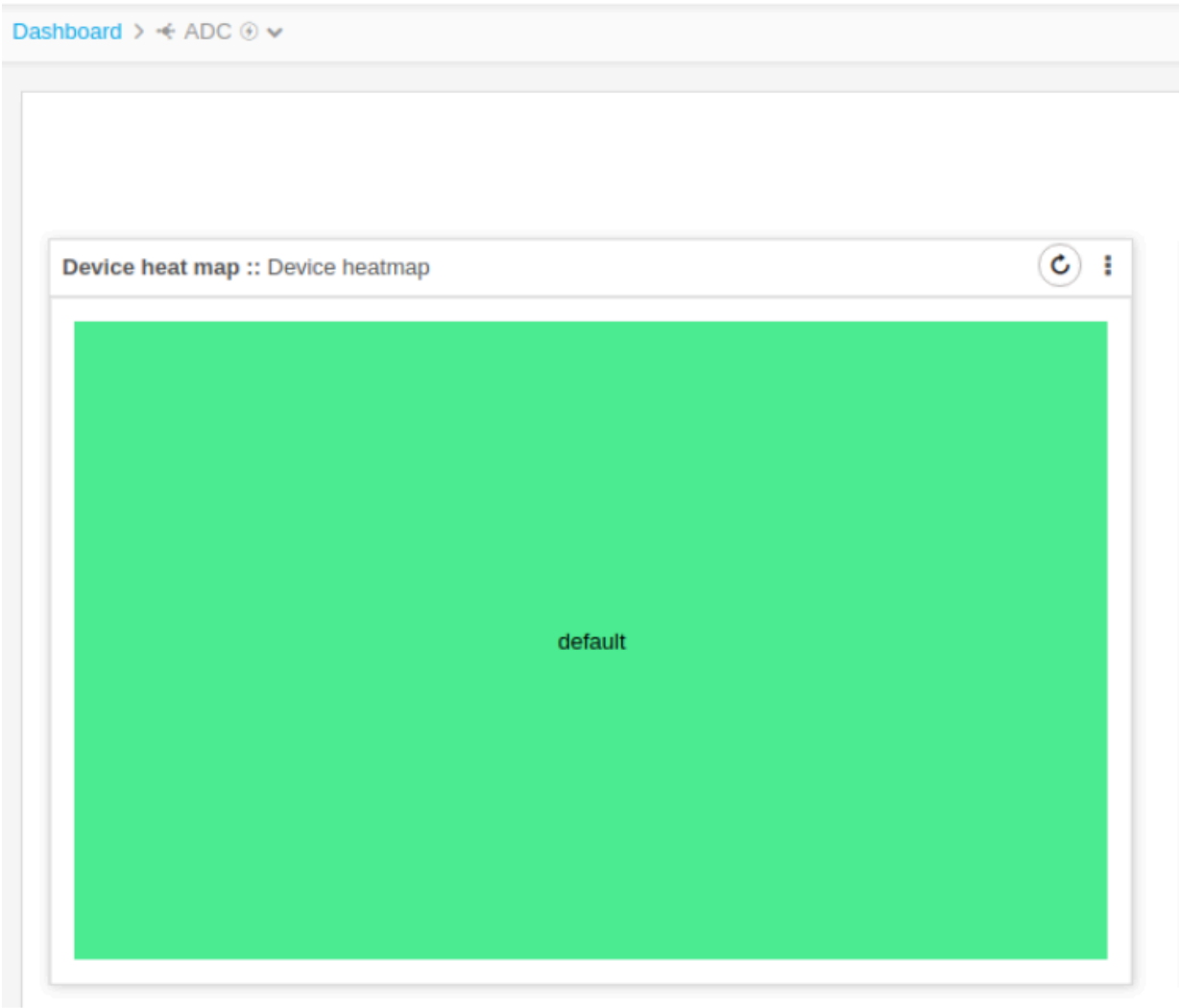
2. From **Dashboard Inventory** click on ADC dashboard.

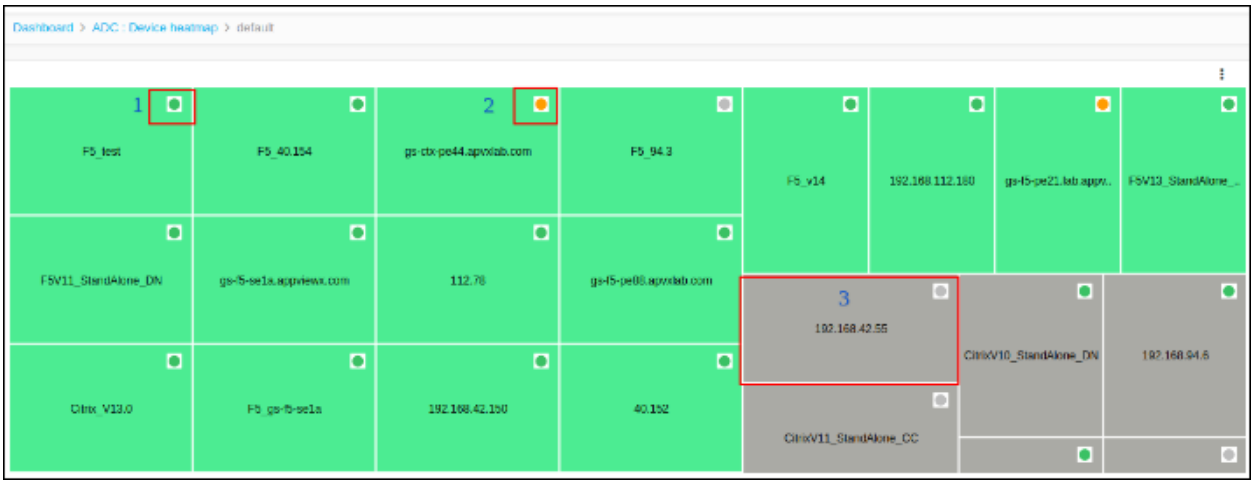
Note: The default widgets can be viewed, aligned, and/or refreshed and not editable.

Widgets in Default Dashboard

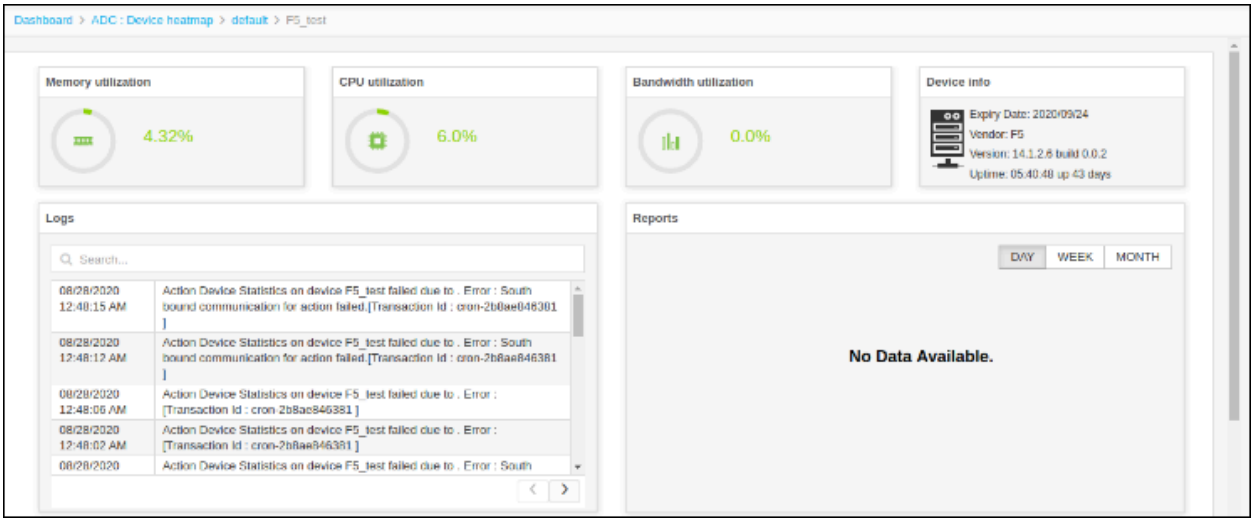
- **Device heat map**

  Device heat map widget shows the CPU utilization, Bandwidth Utilization and Memory Utilization of each device managed in Device Inventory.


Dashboard
ADC
Device heat map :: Device heatmap
default

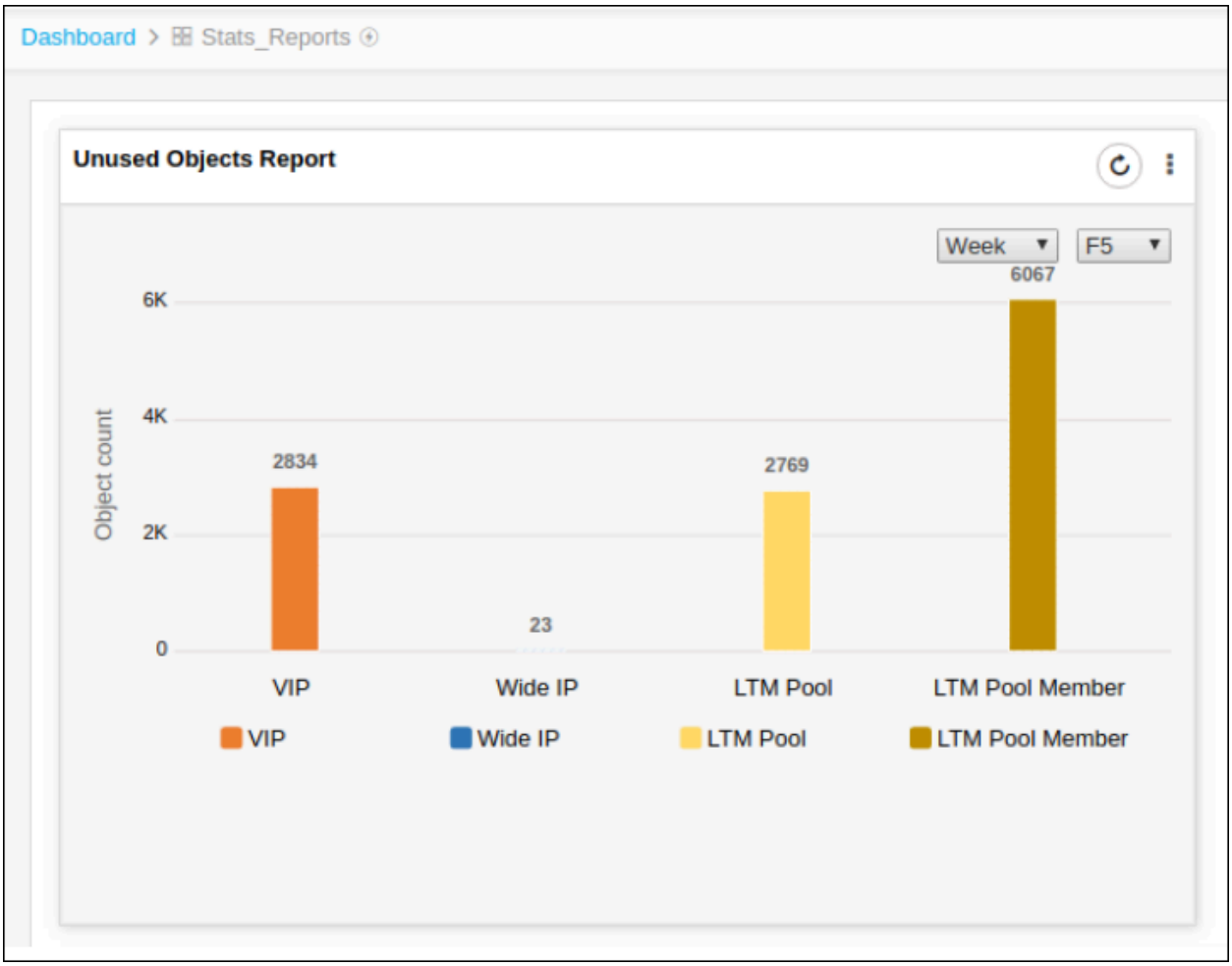

Dashboard > ADC : Device heatmap > default
1
F5_test
F5_40.154
2
gs-ctx-pe44.apvxlab.com
F5_94.3
F5_v14
192.168.112.180
gs-f5-pe21.lab.appv..
F5V13_StandAlone_..
F5V11_StandAlone_DN
gs-f5-se1a.appviewx.com
112.76
gs-f5-pe08.apvxlab.com
3
192.168.42.55
CitrixV10_StandAlone_DN
192.168.94.6
Citrix_V13.0
F5_gs-f5-se1a
192.168.42.150
40.152
CitrixV11_StandAlone_CC

1. Active Device
2. Standby Device
3. Unreachable devices are shown as Grey.
4. Click on the Device and to get detailed information about CPU utilization.



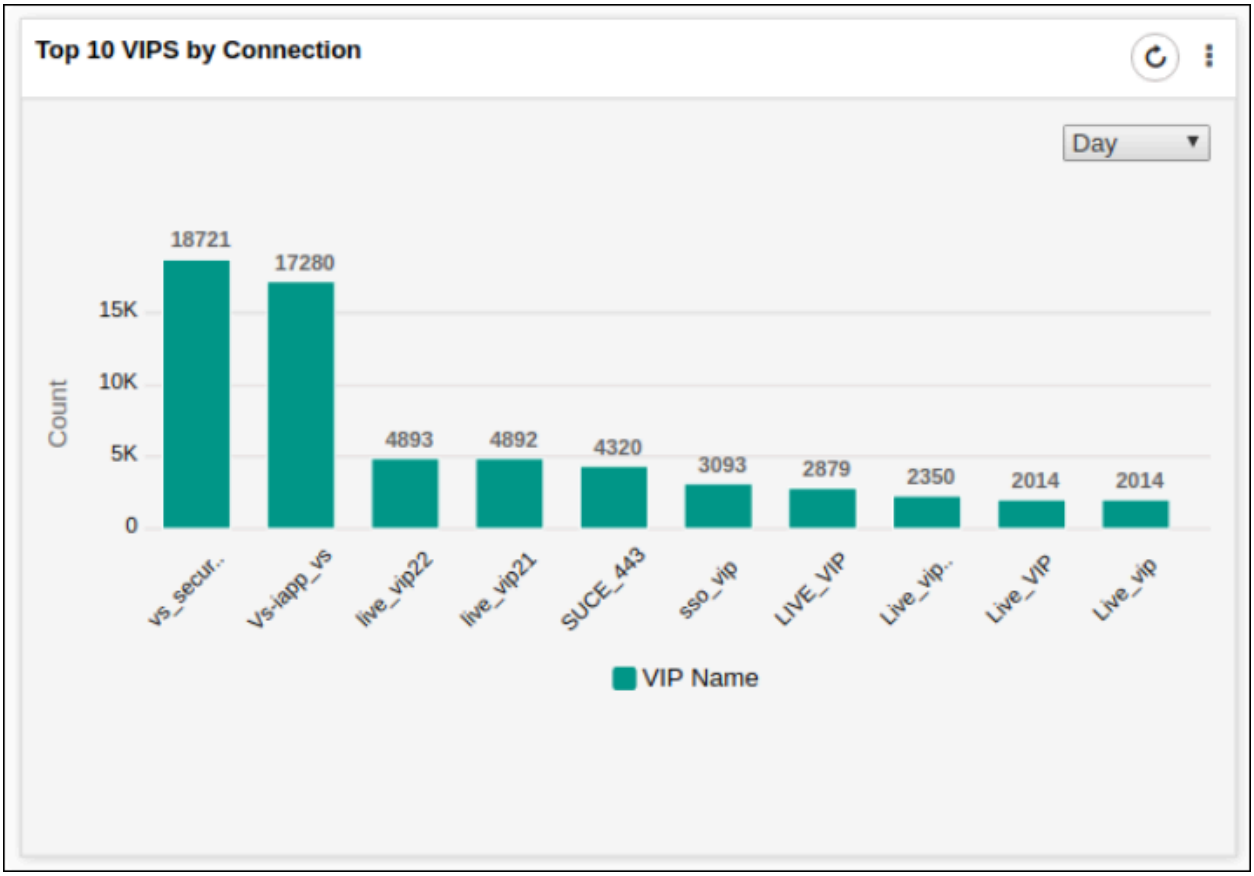
Unused Object Report

Unused Object Report shows the number of unused objects over a period of time. Supported vendors are F5, A10, and Citrix.



Top 10 VIPS by Connection

This widget shows the details about the top 10 VIPs.

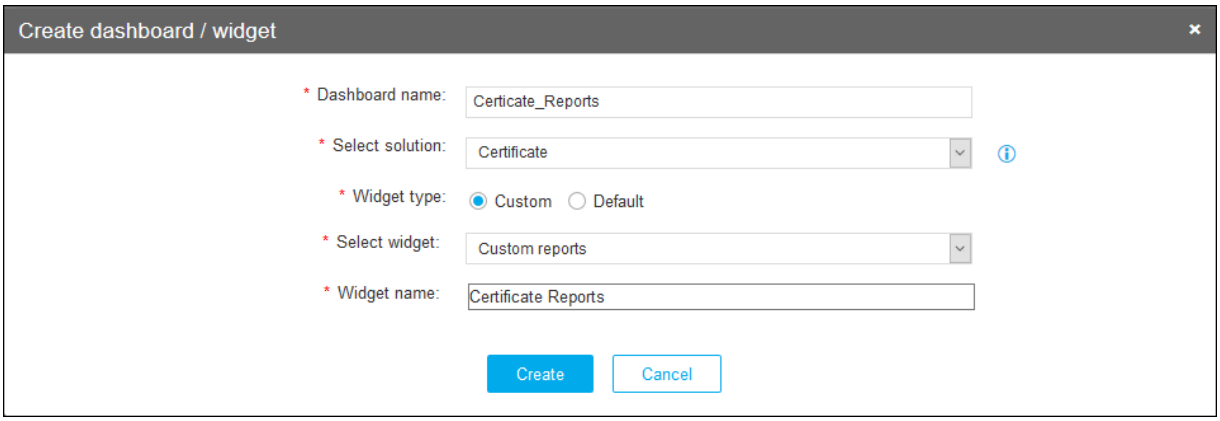


Create a Dashboard/Widget

The custom dashboard allows you to manage, monitor, and interpret all the configured applications and their objects. It provides customizable widgets to get an overview of all the ADC Applications within the AppViewX platform and manage/monitor traffic from a single screen. Customize your Application dashboard with predefined and custom widgets as per the business need. You can create dashboard using any of the following method:

To create a dashboard:

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If this is the first dashboard you are creating in the system, click the Create Dashboard button that appears in the center of the screen. If you have already created at least one dashboard, click (**Create**) icon on the top-right or click (**Create**) icon.
3. On the Create Dashboard/Widget pop-up window, enter a name for the new dashboard.
   The name must not contain spaces in it.



4. Select a solution from the **Select Solution** dropdown to which you want the widget to be created: ADC, Firewall, Certificate, SSH or WAF. Select the solution from the dropdown to which you want the corresponding widgets to be managed: Certificate.
5. Select the **Widget Type** as Custom or Default.
6. If the Custom radio button is selected in Step 5, then choose any one of the below options from the Select Widget dropdown:
   - **Application view** – Allows you to group the service objects of a single application. The widget displays the health of these objects and the number of current connections that the services are receiving.
   - **Traffic statistics** – Displays a chart showing live and historic performance statistics for individual device objects.
   - **Script execution** – Saves script files on a local machine and provides easy access to maintain and execute script commands from within the widget.
   - **Traffic grid** – Allows you to monitor and control the Traffic Percentage of the Applications across data centers. The status, state, and statistics for applications can be viewed through this widget.
   - **Class management** – Allows you to view and modify the classes associated with iRules.
   - **HeatMap** – Allows you to view statistics for managed, failed, and unresolved devices or device groups.
7. If the default radio button is selected in Step 5, choose the default widgets you want to manage/ monitor in the custom dashboard. Select the default widgets you want to manage/monitor in the custom dashboard.
8. Enter a name for the new widget that you will be creating on the dashboard.
9. Click **Create**.
   You are redirected to the widget configuration screen, which varies according to the widget selected.

Note:

- The Settings screen for the new dashboard/widget appears. The contents of the Settings screen vary depending on the type of widget you are adding to your new dashboard.
- All the default dashboards and custom dashboards created are listed in the dashboard inventory.
- If the Auto Sort Dashboards Alphabetically is enabled the dashboards are listed in alphabetical order, if disabled dashboards are listed based on the created order.

Add Widgets

Widget can be created in a new Dashboard or existing Dashboard**.**

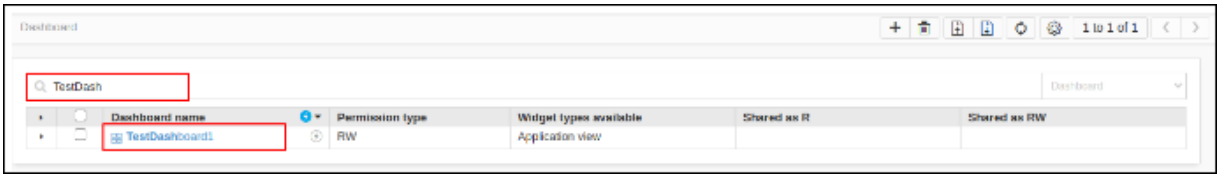
- Application View Widget
- Traffic Statistics Widget
- Script Execution Widget
- Traffic Grid Widget
- Class Management Widget

Add Widget in New Dashboard

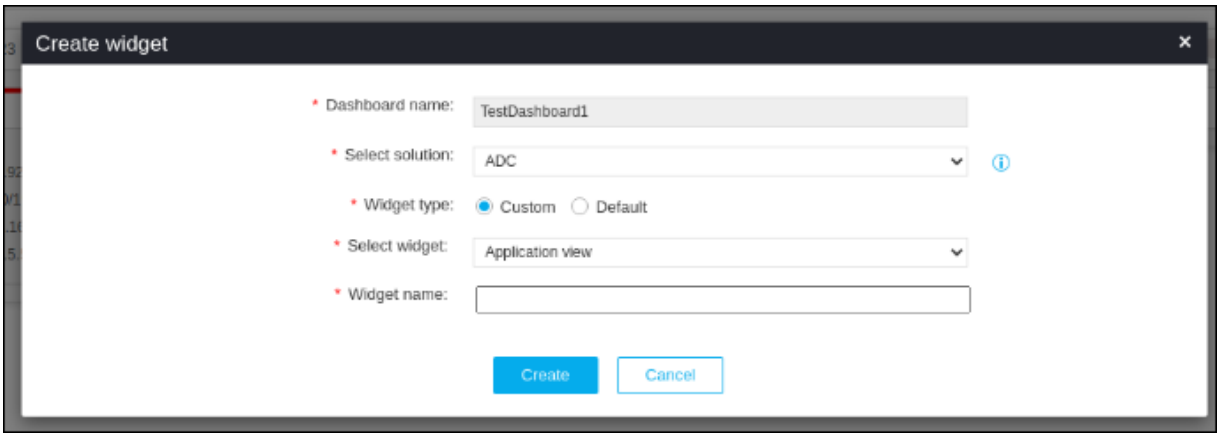
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** >**Dashboard** > Click on **Plus** icon.

Add Widget in Existing Dashboard

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Dashboard**.
3. Search for the Dashboard from dashboard inventory and Click on the dashboard name add a new widget.



4. Click Add Widget icon.



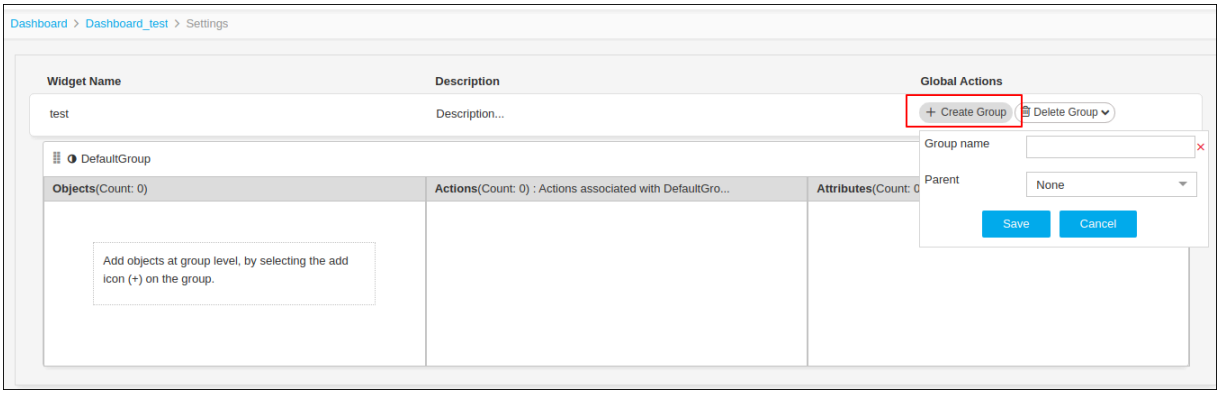
5. Select Widget Type and provide Widget name.
   Based on the selected widget type, the corresponding widget settings page is loaded.

Application View Widget

Using Application View Widget , the ADC Primary objects like Wideip, GTM Pool, Virtual servers, LTM Pool and nodes can be monitored for state and status change and Actions can be performed. The actions for each object is predefined and can be selected accordingly.

To Create a Group

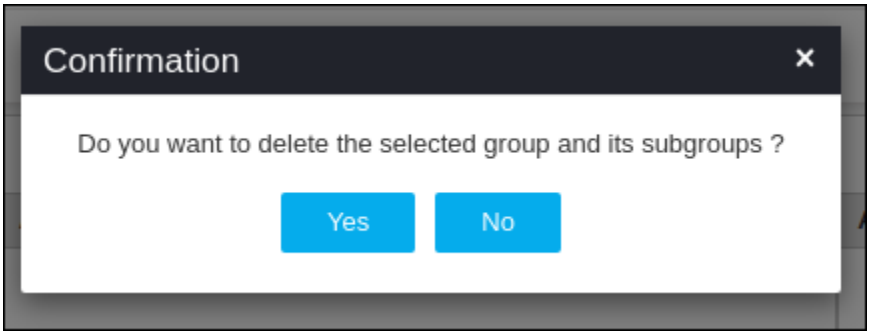
1. Click on Create Group
2. Provide a user defined group name
3. Parent group can also be selected from the list of available groups added in the widget.
4. Maximum group hierarchy allowed is four.



To Delete a Group

1. Click Delete Group and select the groups to be deleted.

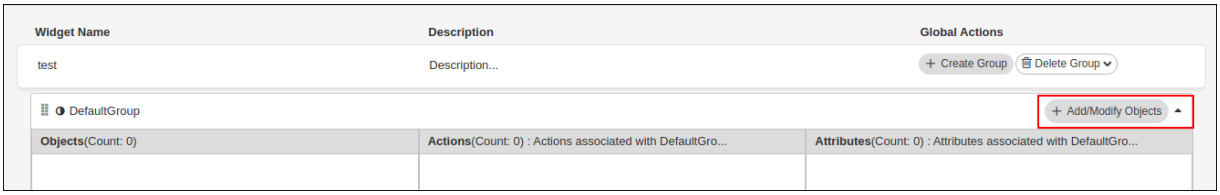
> **CAUTION:** The groups will be deleted with all subgroups and it's configured objects.

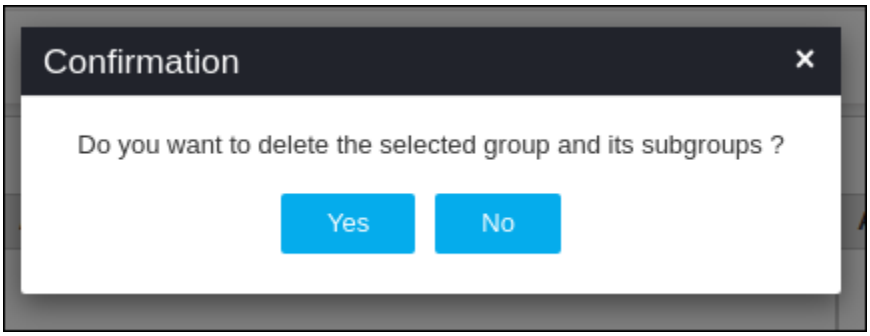


2. Click yes on the confirmation to proceed the deletion.

To Add/Modify Objects in a Group

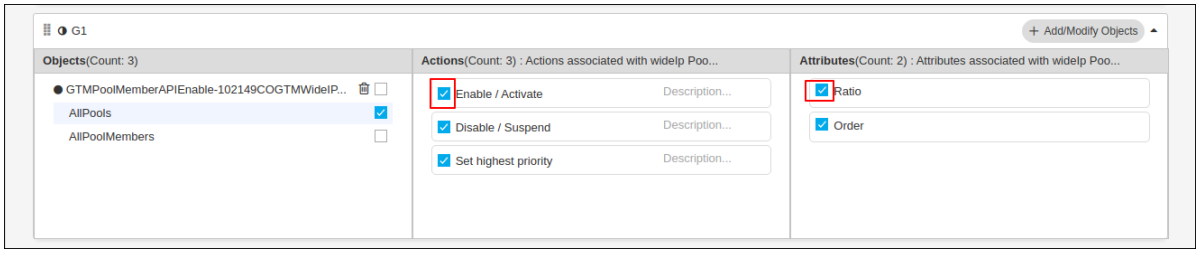
1. Click Add/Modify objects on the Default/Created Group



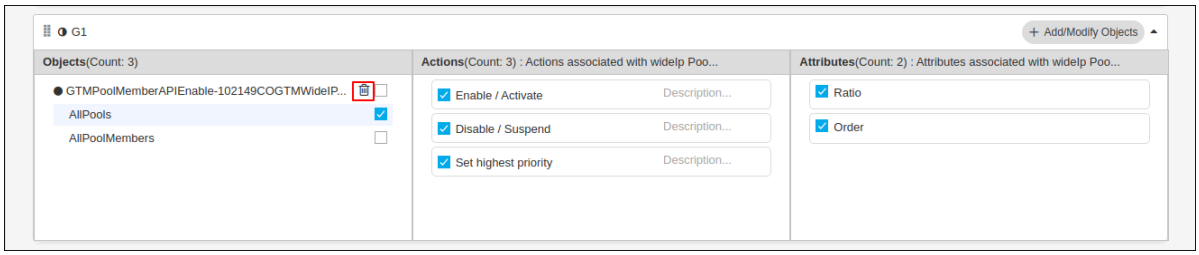


Name	Type	Mandatory	Description	Validation
Vendor	Drop Down	Yes	Vendors of Managed devices from the inventory are listed in Alphabetical order.	NA
Device State	Drop down	Yes	Available options: **Active** : Active devices are listed. **Standby** : Standby devices are listed. **All** : All Managed devices are listed.	NA
Device Name	Drop Down	Yes	Based on vendor and device state, available devices are listed.	NA
Object Type	Drop Down	Yes	Based on the vendor, all supported object types are listed.	NA
Hierarchy	Drop Down	Yes	Based on the Object Type selected the hierarchy is listed.	NA

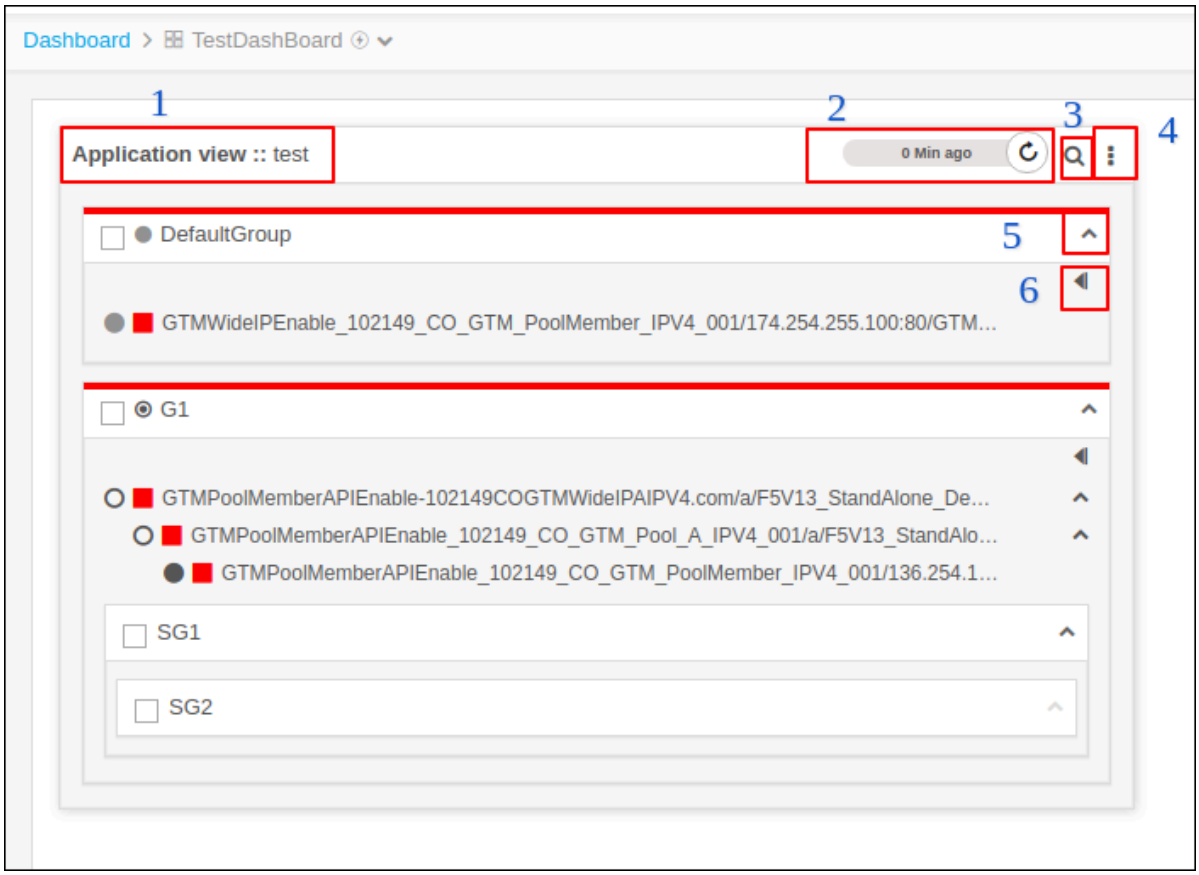
• Based on the objects added, Default actions are selected. Users can deselect the actions



• To Delete added objects in a Group, click on the delete symbol next to the object.



- Once the configuration is completed an Test Widget would displayed. The test widget contains the following:



a. Widget Name

b. Last refresh time, when the widget is refreshed,the current state and status are fetched from the device and updated in the widget

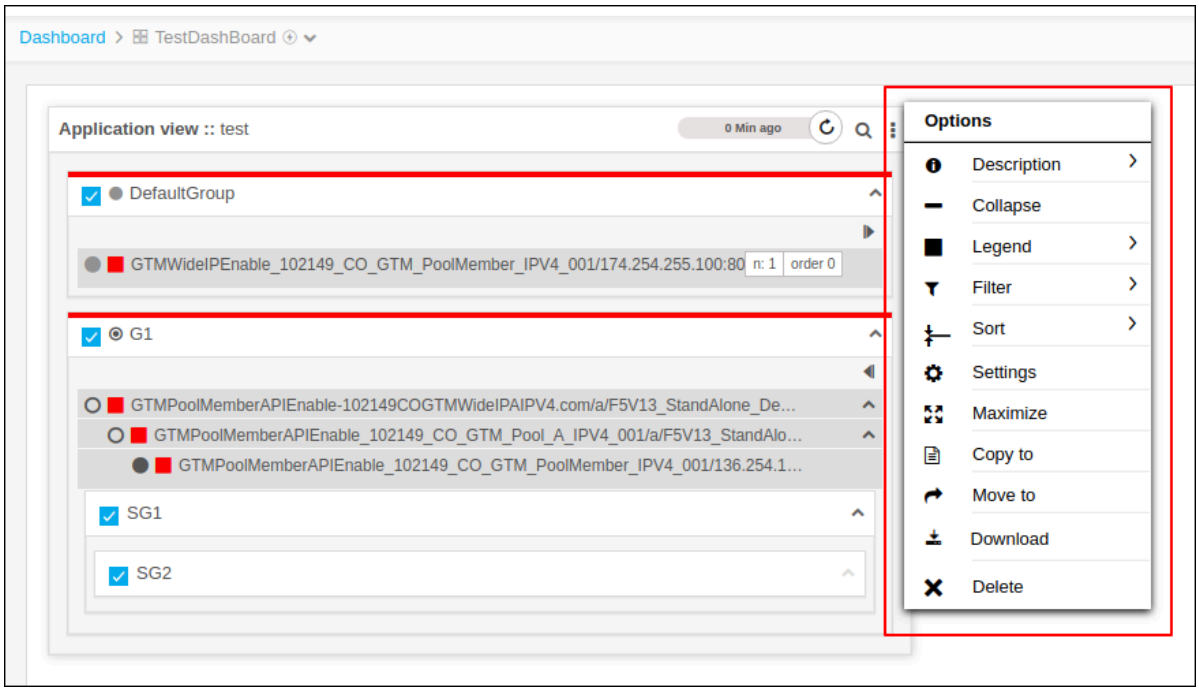
c. To search for an object added in the widget

d. Settings options

e. Collapse/Expand the Group

f. To display the attributes of the objects

Widget Settings:

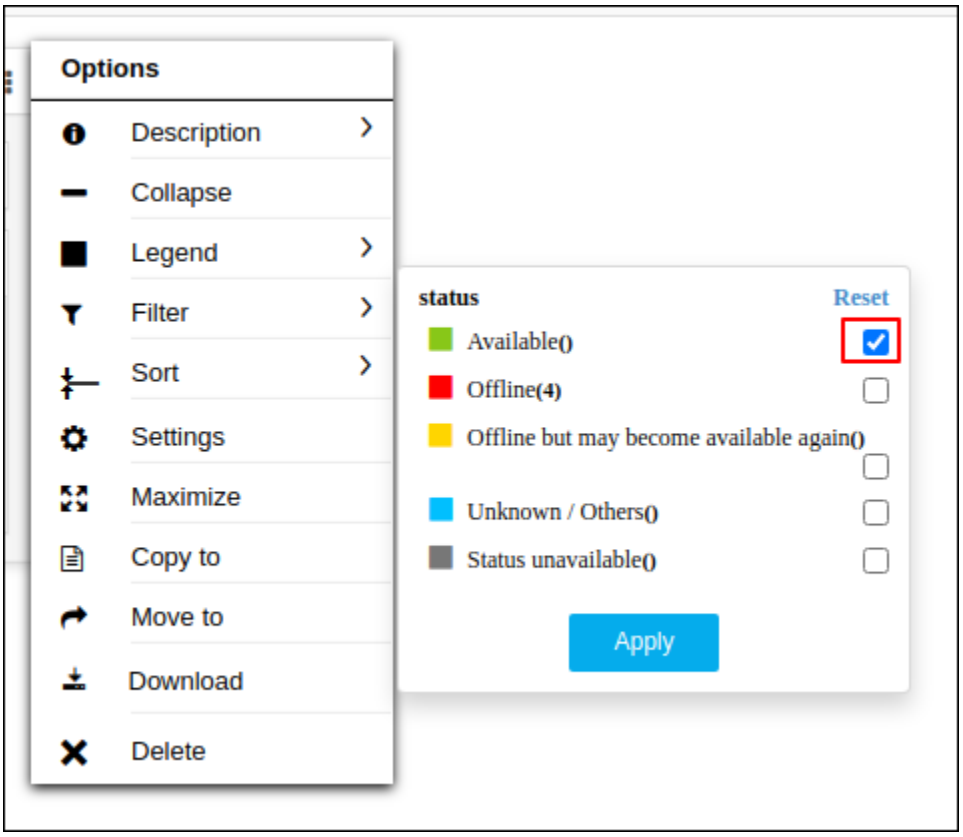


a. Description - Description provided for the widget while creating it.

b. Collapse/Expand the Widget

c. Legend - Gives information about representations used in Widget.

d. Filter - Filter the objects to be shown based on status and Click Apply.



e. Sort - To Sort the objects in Ascending/Descending order

f. Settings - Settings page of the widget

g. Maximize - To Maximize the widget

h. Copy to - The widget is copied to another Dashboard.

i. Move to - The widget is moved to another Dashboard.

j. Download - Download the widget as csv file

k. Delete -to delete the widget

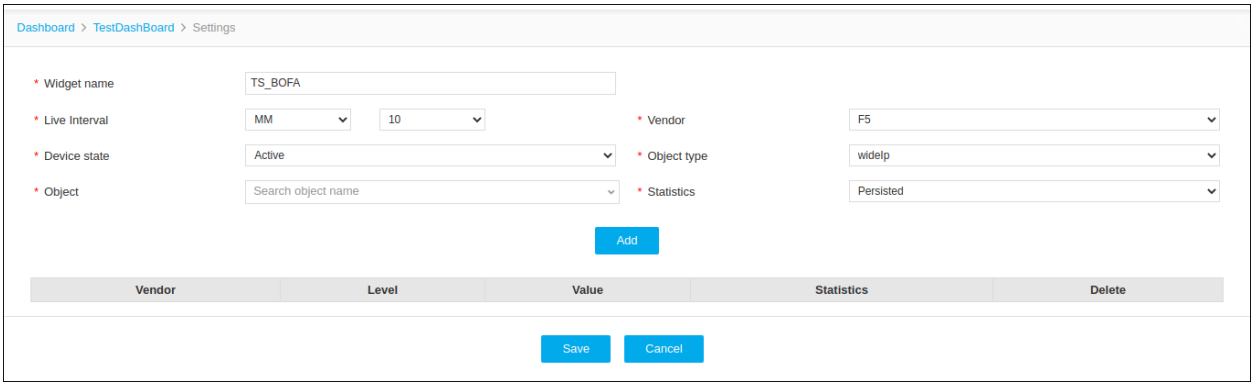
2. Based on the above filters, available objects are listed. Specific objects can also be searched and added.
3. Select the objects to be added and click ADD.

Actions on Objects/Groups

Right click on Object/Groups and actions are displayed based on the object type and ACF permissions assigned to the user.

Traffic Statistics Widget

Traffic statistics widget is used to monitor live/historic statistics of objects.

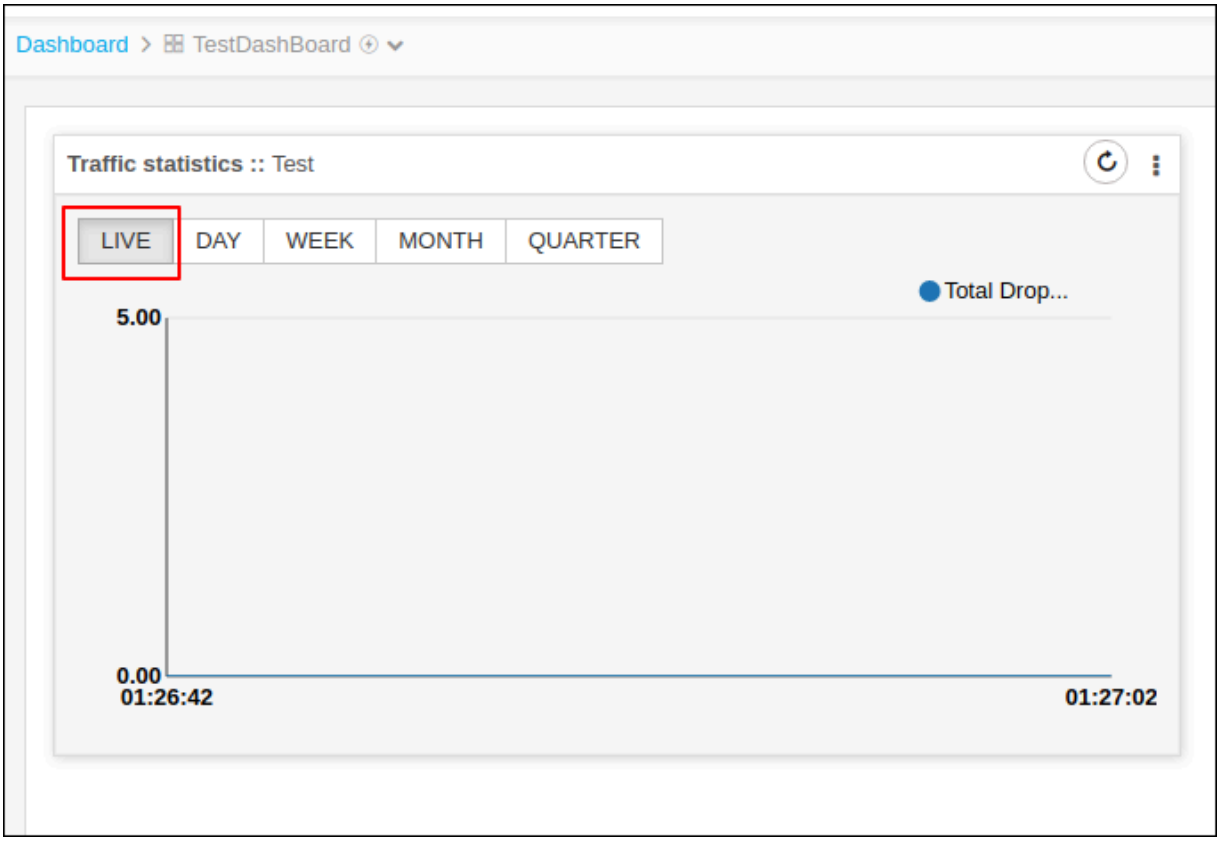


1. Add objects

Name	Type	Mandatory	Description	Validation
Widget Name	Text box	Yes	User defined Name for the Widget	No special characters are allowed, except '_' , '.' , '-' , '|' , ':'. The name should not start with a special character.
Live Interval	Drop Down	Yes	Set time interval for live statistics collection.	NA
Vendor	Drop Down	Yes	Statistics supported Vendors are listed	NA
Device State	Drop down	Yes	Available options: **Active** : Active devices are listed. **Standby** : Standby devices are listed. **All** : All Managed devices are listed.	NA

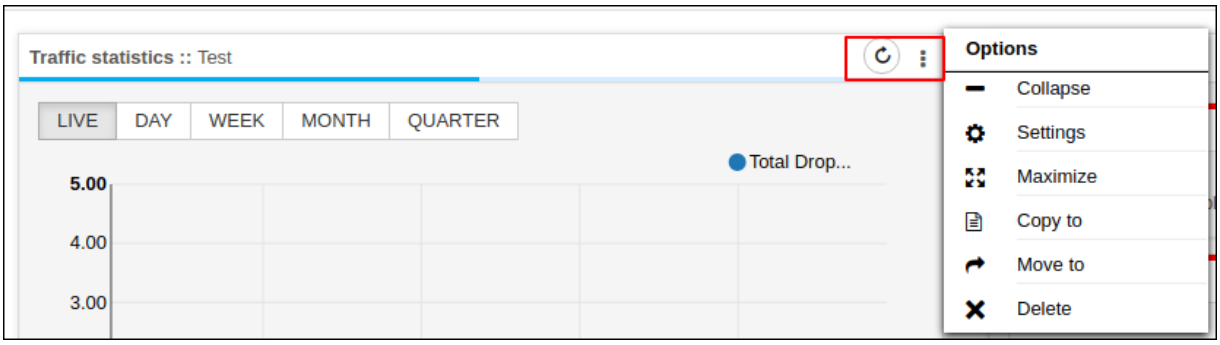
Name	Type	Mandatory	Description	Validation
Object Type	Drop Down	Yes	Based on the vendor, all supported object types are listed.	NA
Object	Drop Down	Yes	Based on vendor and object type filter available objects are listed.	NA
Statistics	Drop Down	Yes	Based on vendor and object type filter supported statistics parameters are listed.	NA

2. Provide the required information and click Add.
3. Click Save



By default Live stats are collected. If Insight is enabled then historic statistics are shown.

Widget Setting:



a. Refresh - Refreshing the widget will get live stats for the configured objects.

b. Collapse/Expand - Collapse and expand the widget screen

c. Settings - Configure the settings

d. Maximize - To maximize the widget size

e. Copy to - The widget is copied to another dashboard

f. Move to - The widget is moved to another dashboard.

g. Delete - Delete the widget

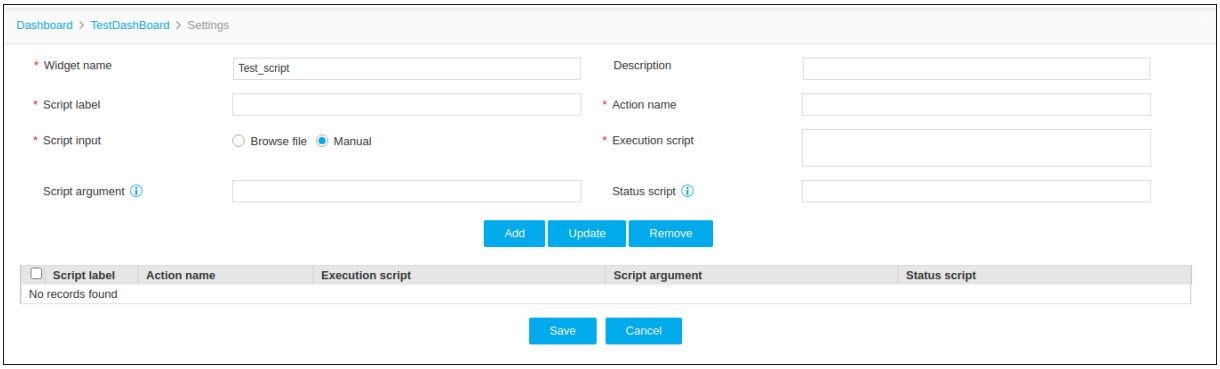
Script Execution Widget

Using Script Execution Widget, scripts which can be executed within 5 minutes can be configured and executed.

Before you begin: Set Timeout in system Settings. Refer Configuring Script Execution Settings

Configuring Script Execution Widget

1. Add Scripts



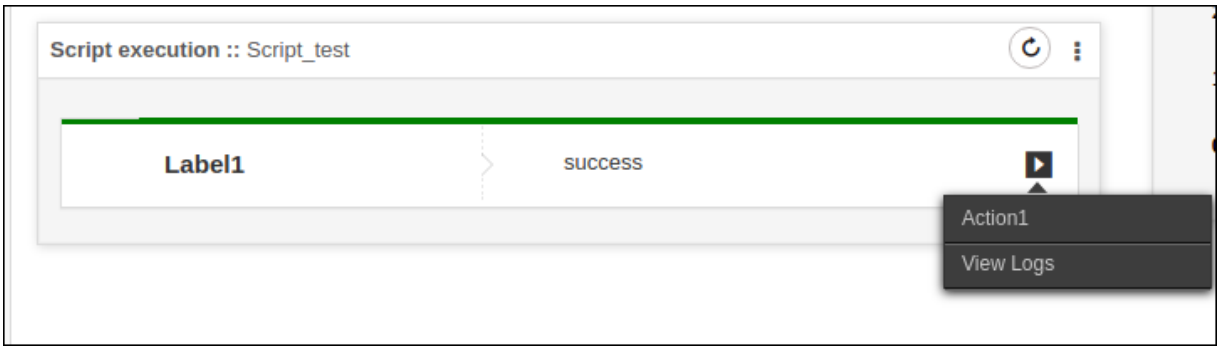
2. Provide information

Name	Type	Mandatory	Description	Validation
Widget Name	Text box	Yes	User defined Name for the Widget	No special characters are allowed, except '_' , '.' , '-' , '|' , ':'. The name should not start with a special character.
Description	Text box	No	Description for the Widget	-
Script label	Text box	Yes	-	-
Action Name	Text box	Yes	-	-
Script Input	Radio button	Yes	**Browse file:** Script file can be uploaded. **Manual:** Script can be typed in the text box.	NA
Execution Script	Text box	Yes	1.File can be uploaded. or 2. Manual script input can be added.	NA
Script argument	Text box	No	Arguments for the script can be mentioned with space as delimiters.	-
Status script	Text box	No	The full path of the scripts in AppViewX servers to update the color and status message of the bar. This functionality is used to get the status/ result of a script.	-

3. After adding all information, click **Add** and **Save**

Execution of Scripts

1. Click on the Play icon and click on the Action Name configured.

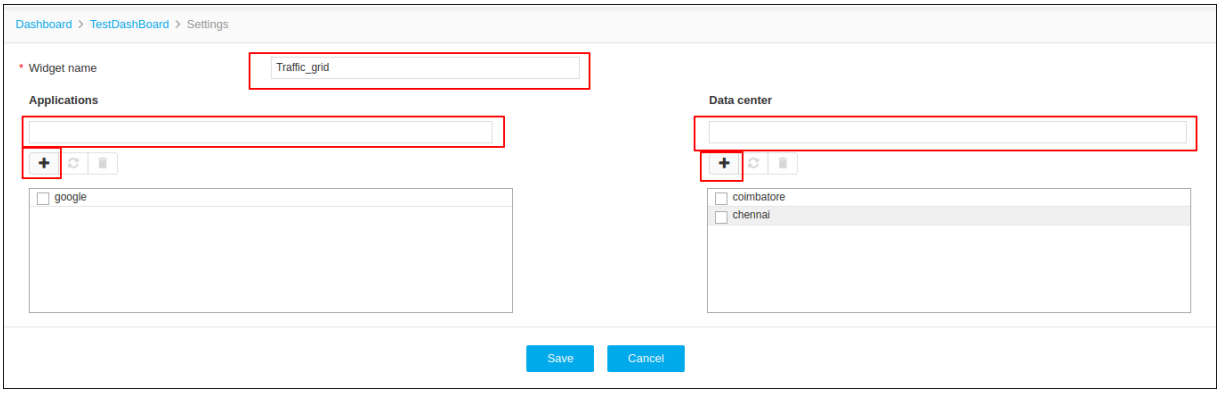


2. Output logs can be verified using View Logs option.

Traffic Grid Widget

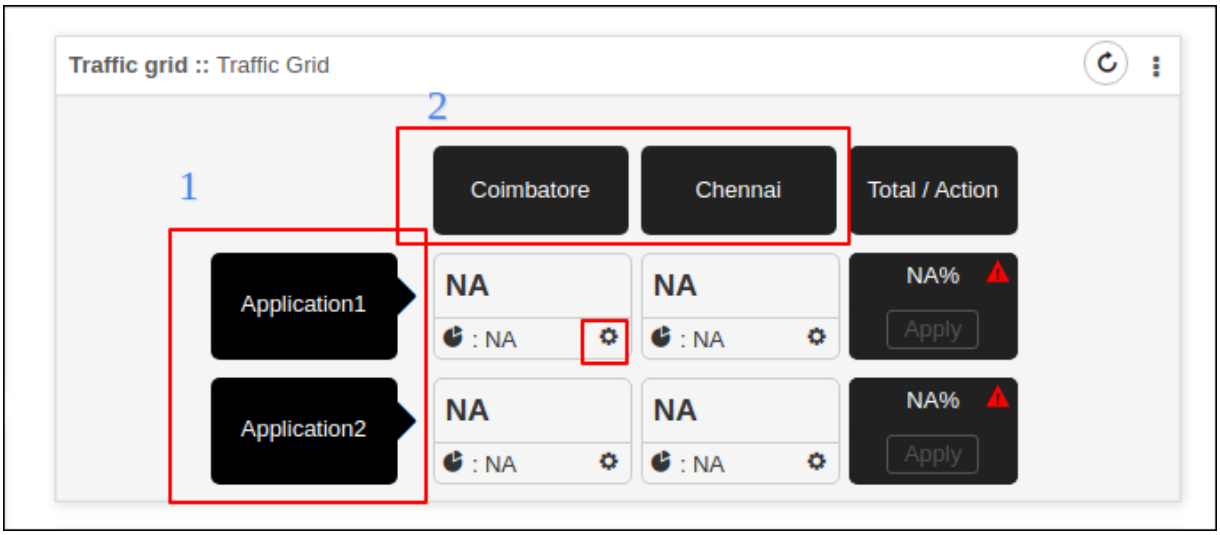
Configuration Steps:

1. Provide widget name



2. Add Application Name and Data Centers and click on Add icon
3. Click **Save**

   Sample Widget



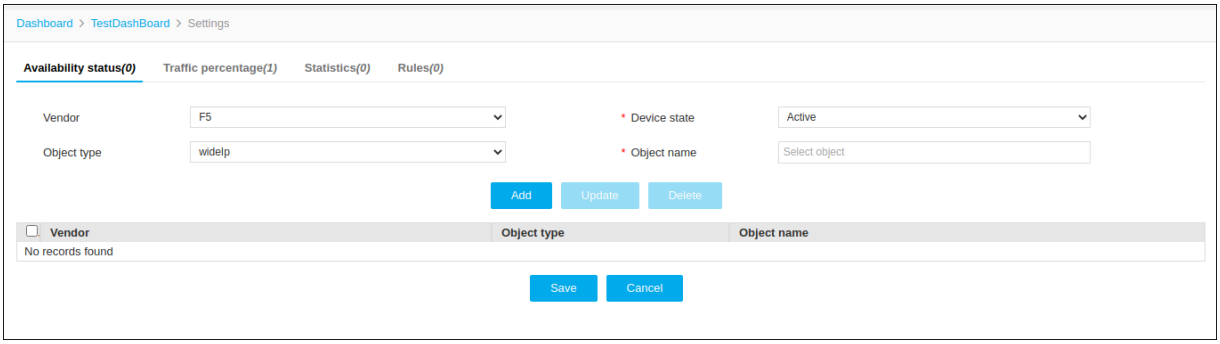
a. Applications Configured

b. Data Centers added

c. Click on Settings icon to configure objects and rules

1. Configure Availability Status

1. Provide required information

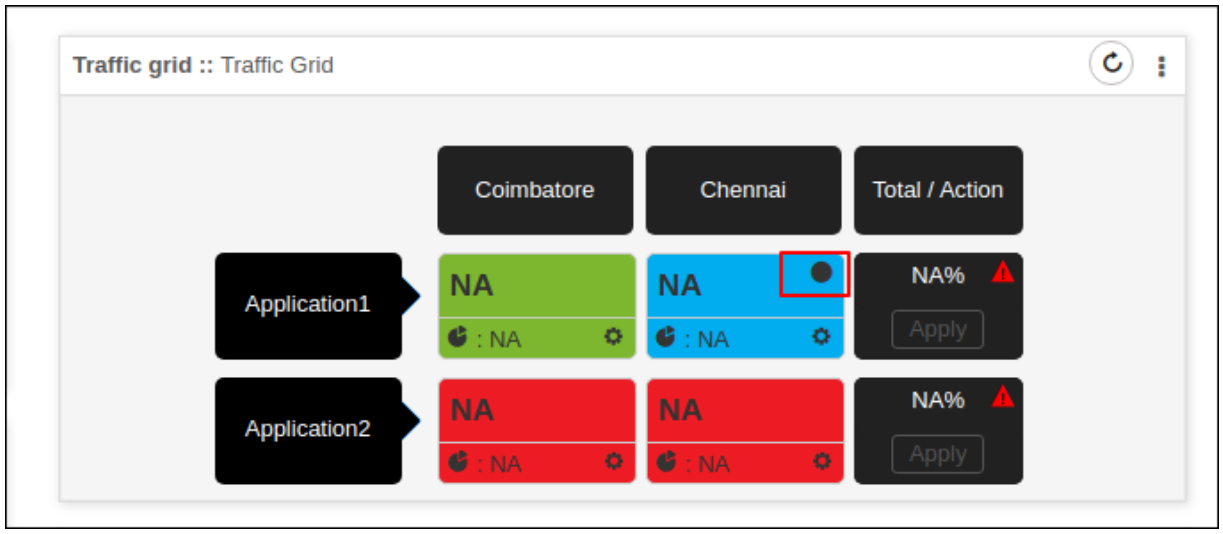


Name	Type	Mandatory	Description	Validation
Vendor	Drop Down	Yes	Select vendor	NA
Device State	Drop Down	Yes	Available options: **Active** : Active devices are listed. **Standby** : Standby devices are listed.	NA

Name	Type	Mandatory	Description	Validation
			All : All Managed devices are listed.	
Object type	Drop Down	Yes	All Primary ADC objects are listed.	NA
Object Name	Drop Down	Yes	Object names can be searched and selected.	NA

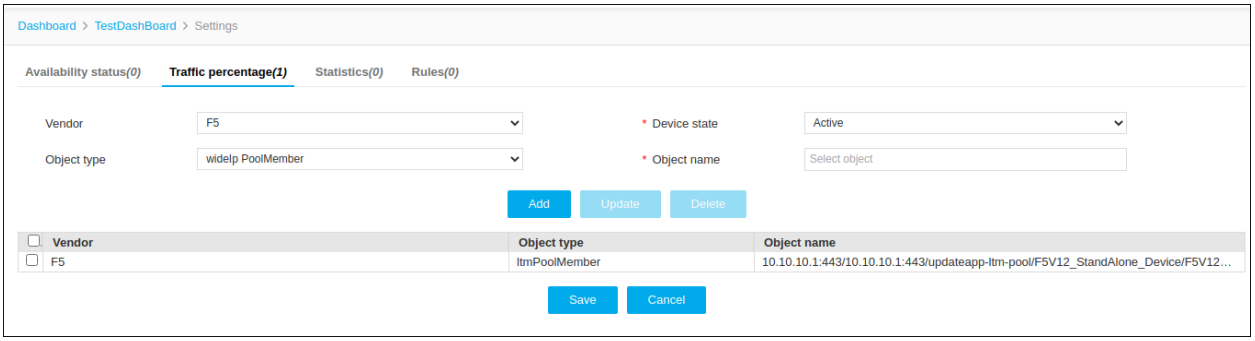
2. Click **Add** and **Save**
3. Added objects can also be updated by selecting the object in the list and **Update**
4. Added Objects can be deleted by selecting the object in the list and **Delete**

   After configuring the objects the color representation changes according to status of the objects and State of the objects are also represented at top right corner of every application.



2. Configure Traffic Percentage

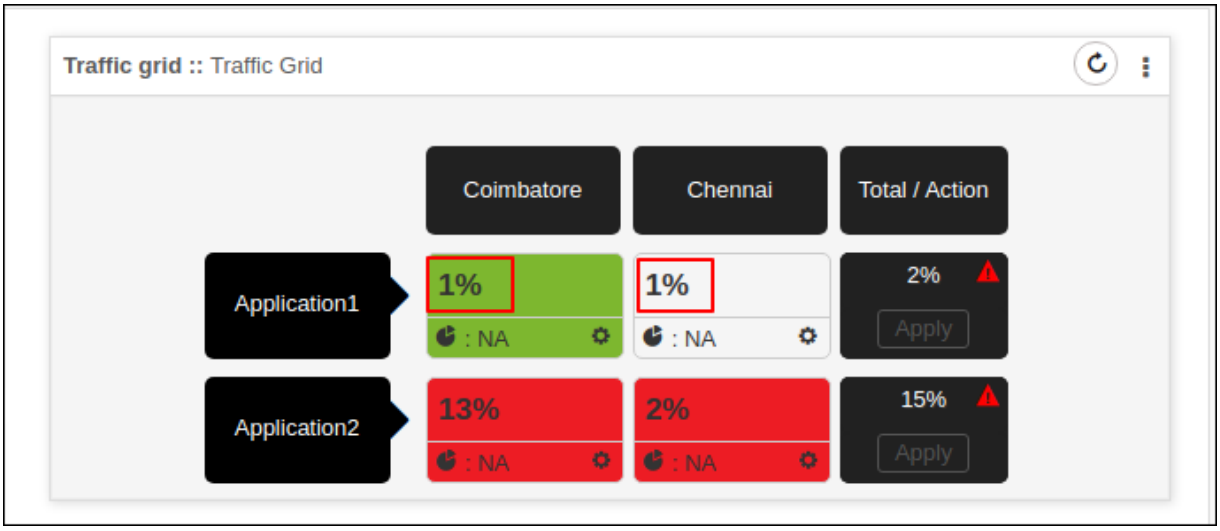
By adding objects in traffic percentage, users can route the traffic by changing the traffic percentage.



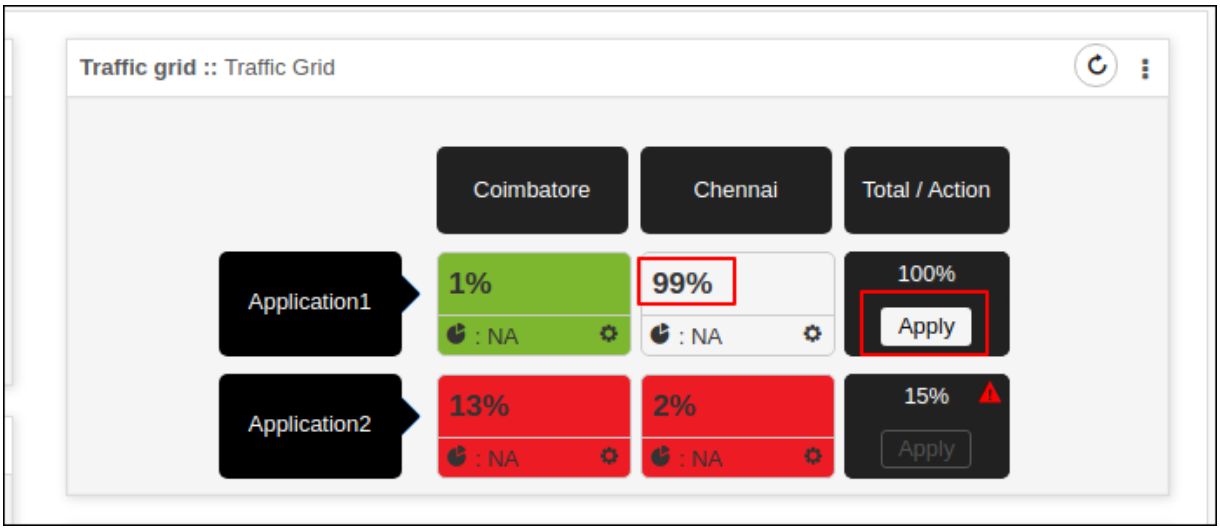
1. Provide required information

Name	Type	Mandatory	Description	Validation
Vendor	Drop Down	Yes	Select vendor	NA
Device State	Drop Down	Yes	Available options: **Active** : Active devices are listed. **Standby** : Standby devices are listed. **All** : All Managed devices are listed.	NA
Object type	Drop Down	Yes	Only traffic controllable objects like pool members are listed	NA
Object Name	Drop Down	Yes	Object names can be searched and selected.	NA

2. Select the objects and Click Add.
3. After adding the traffic percentage value is shown on the widget.



4. Traffic percentage values can be altered and Applied on the objects.

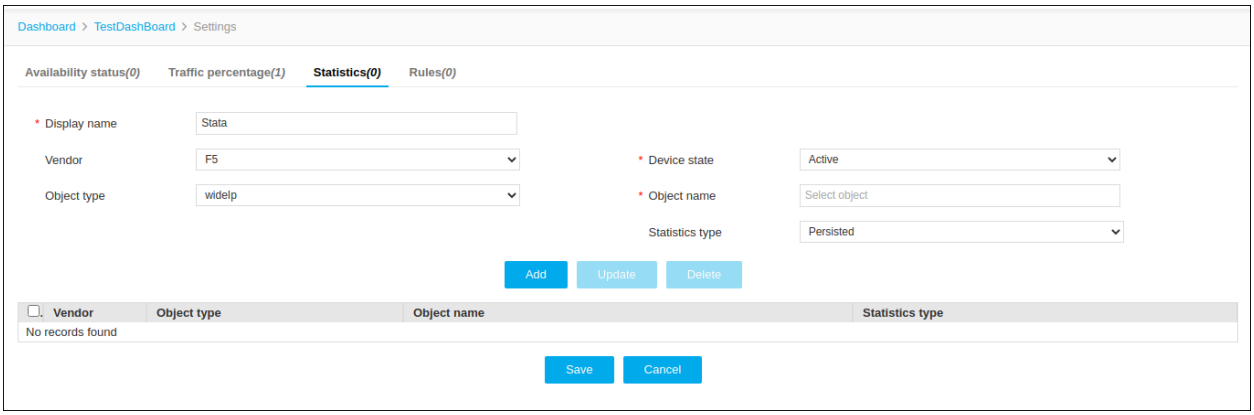


5. Modify the traffic percentage and click Apply to execute action on the objects added.

> **Note:** The sum of all traffic percentages should be 100.

3. Configure the Statistics

By adding objects in the statistics tab, stats for added objects can be monitored.

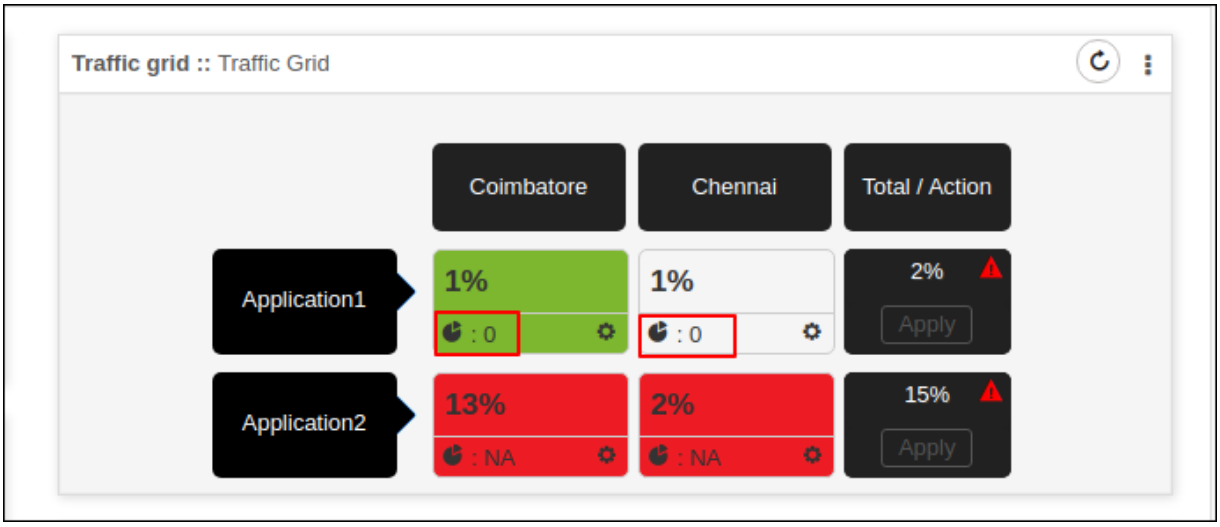


1. Provide required information

Name	Type	Mandatory	Description	Validation
Display Name	Text Box	Yes	User defined name for stats to be displayed	Only 10 characters are allowed.

Name	Type	Mandatory	Description	Validation
Vendor	Drop Down	Yes	Select vendor	NA
Device State	Drop Down	Yes	Available options: **Active** : Active devices are listed. **Standby** : Standby devices are listed. **All** : All Managed devices are listed.	NA
Object type	Drop Down	Yes	All Primary ADC objects are listed.	NA
Object Name	Drop Down	Yes	Object names can be searched and selected.	NA
Statistics Type	Drop Down	Yes	Statistics parameters for selected object type are listed.	NA

2. Stats collected for the configured objects are displayed in the widget



4. Add Rules For Action

1. **Configure Warning for an action**

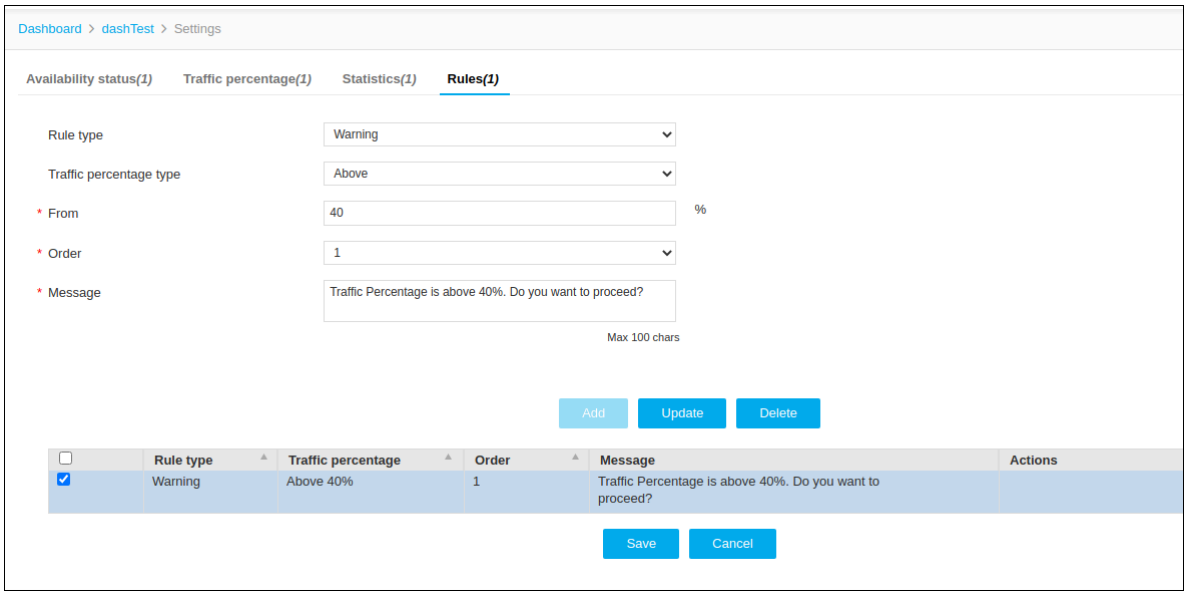
   a. Select Rule type as Warning.

   b. Set the condition to be checked.

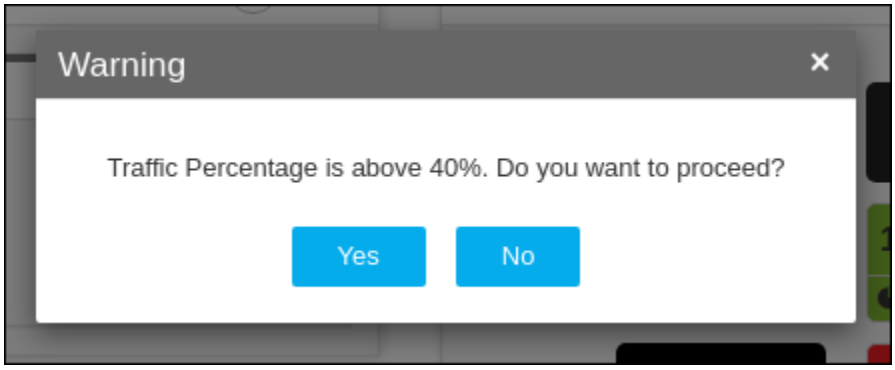
c. Set the order of execution. Maximum 10 rules can be configured.

d. Provide a warning message to be displayed when the condition becomes true.

e. Click **Add** and **Save**.



On performing action , the warning message is displayed when the condition is true.



2. **Configure Restriction for an action**

a. Select Rule type as Restriction.

b. Set the condition to be checked.

c. Set the order of execution. Maximum 10 rules can be configured.

d. Provide a Restriction message to be displayed when the condition becomes true.

e. Click **Add** and **Save**.

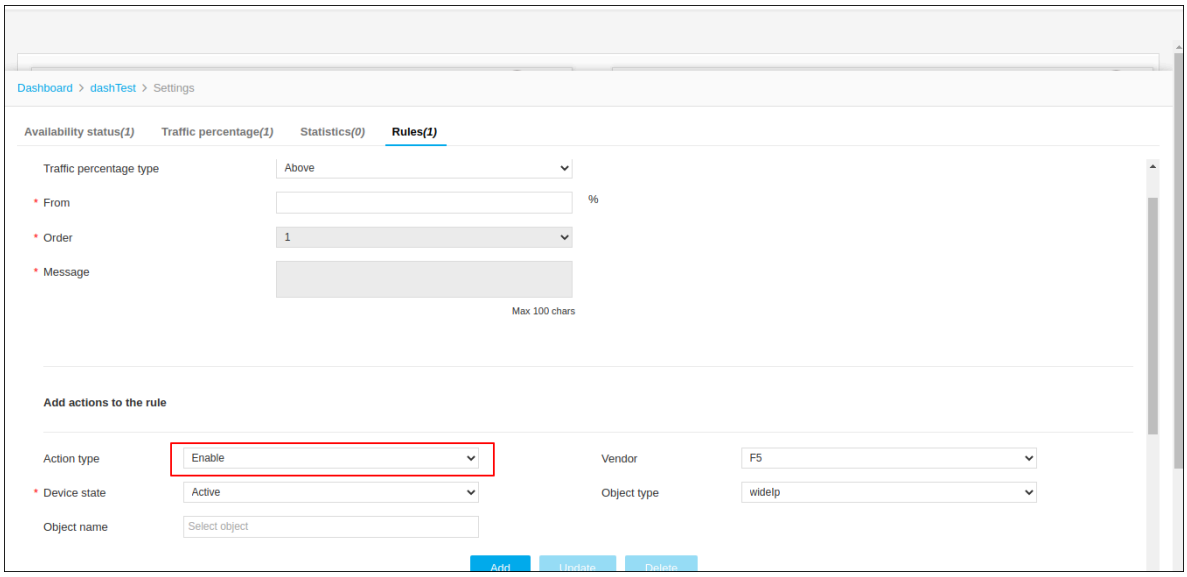
Adding restrictions will not allow the user to perform the action.

3. **Configure action when certain condition met**

   a. Select Rule type as Action.

   b. Set the condition to be checked.

   c. Configure Enable/Disable action on objects.



   d. Select the Action Type and the object on which action has to be executed.

   e. Click **Add** and **Save**.

   When the condition becomes true, the configured action is executed on the object.

Class Management Widget

Class management widget is used to execute actions on the Data group of F5 devices. The data group values can be Viewed and Modified.

Configuration

Provide the information

Name	Type	Mandatory	Description	Validation
Widget Name	Text box	Yes	User defined Name for the Widget	No special characters are allowed, except '_' , '.' , '-' , '|' , ':'. The name should not start with a special character.

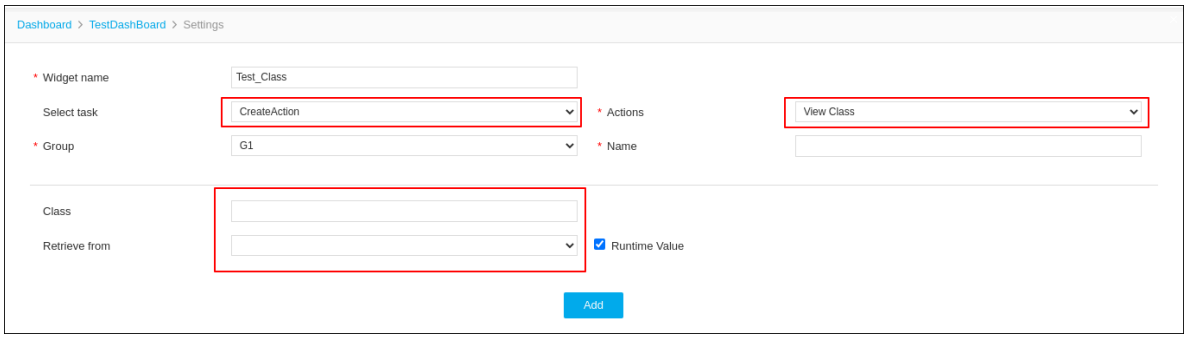
Name	Type	Mandatory	Description	Validation
Select task	Drop Down	Yes	**1.Create Group** Create a new Group.Default Group would be the Widget name. **2.Modify Group** Modify the groups added. **3.Create Action** Create View/Modify action **4.Modify Action** Modify the configured actions.	NA
Group	Drop Down	Yes	List of groups added in the Widget.	NA
Name	Text box	Yes	User defined name for Groups/Actions.	NA

Create Group

Select task as Create Group and Provide a Group name and Click **Add**.

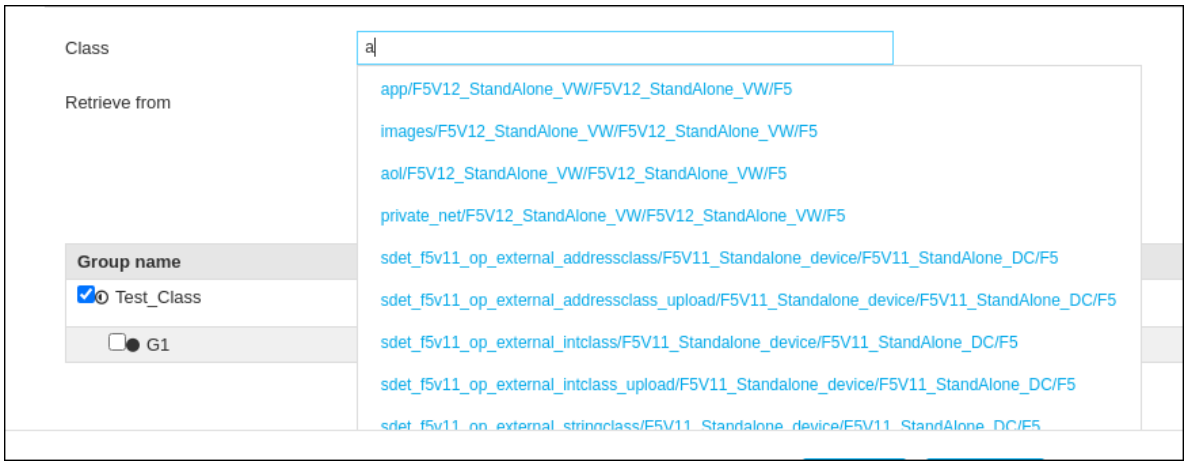
Create Action

1. **View Class**
    a. Select task as Create Action.
    b. Select View Class in Actions.
    c. Select the group and provide Action Name.



d. Search the data group name in Field Class.

The list of devices are listed in Retrieve From.



e. Select the data group and Click **Add** and **Save**.

2. **Modify Class**

a. Select task as Create Action

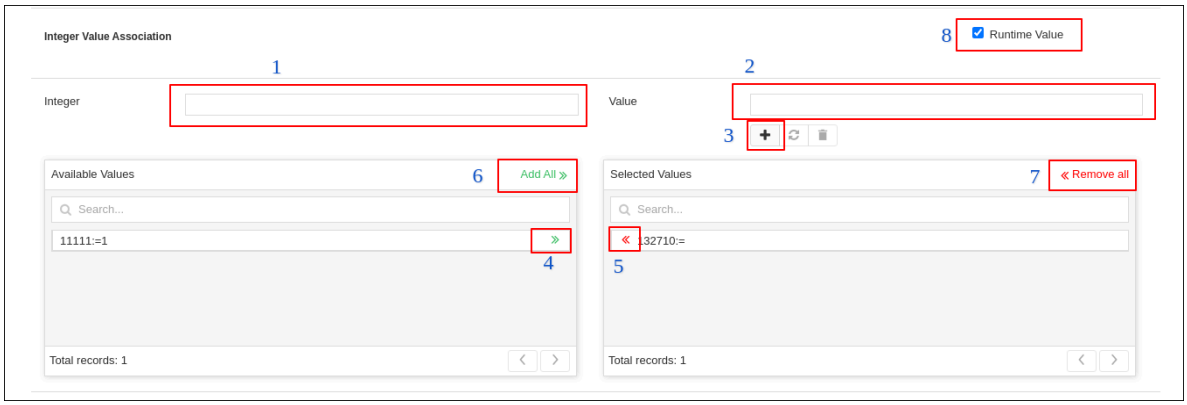
b. Select Modify Class in Actions.

c. Select the group and Provide Action name.

d. Search the data group name in Field Class.

The list of devices are listed in Retrieve From.

e. Add Attributes to be added in the datagroup.



f. Add Key

g. Add Value

h. Click on the Add icon. The added pair is moved to Available Values.

i. In Selected Values, attributes available in the device are listed.

j. Using Add/Remove and AddAll/Remove All Arrows, attributes can be modified.

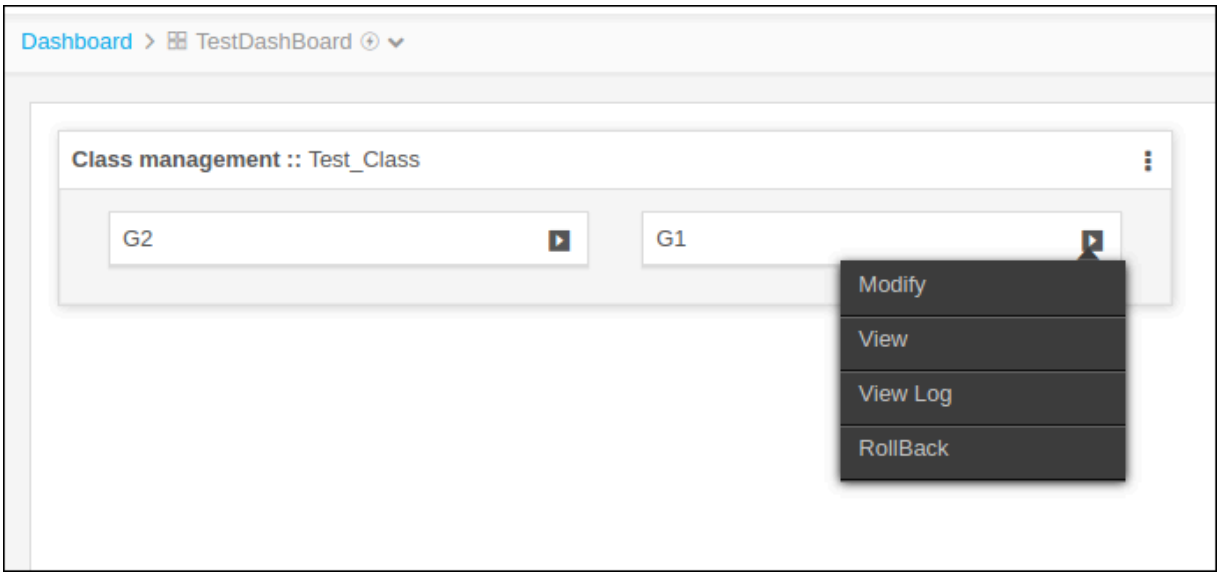
k. Selecting Runtime value allows to modify the attributes at the time of execution.

l. Select the devices on which the action has to be executed.

m. Click **Add** and **Save**.

Execution of Configured Actions

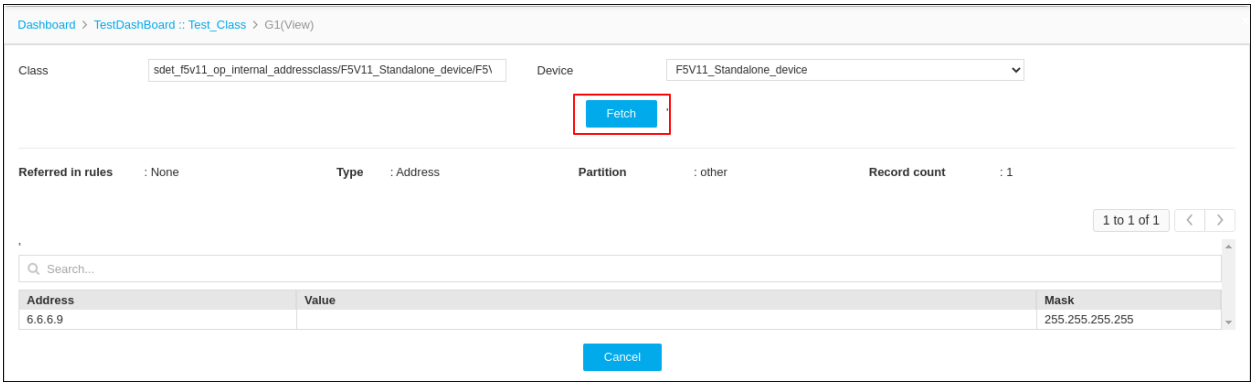
1. Click on the Play icon on the Group.



2. Click on the Action name to be Executed.

View Action Execution

View Action will get the data group attributes from the device.Click on Fetch to get current values from the device.

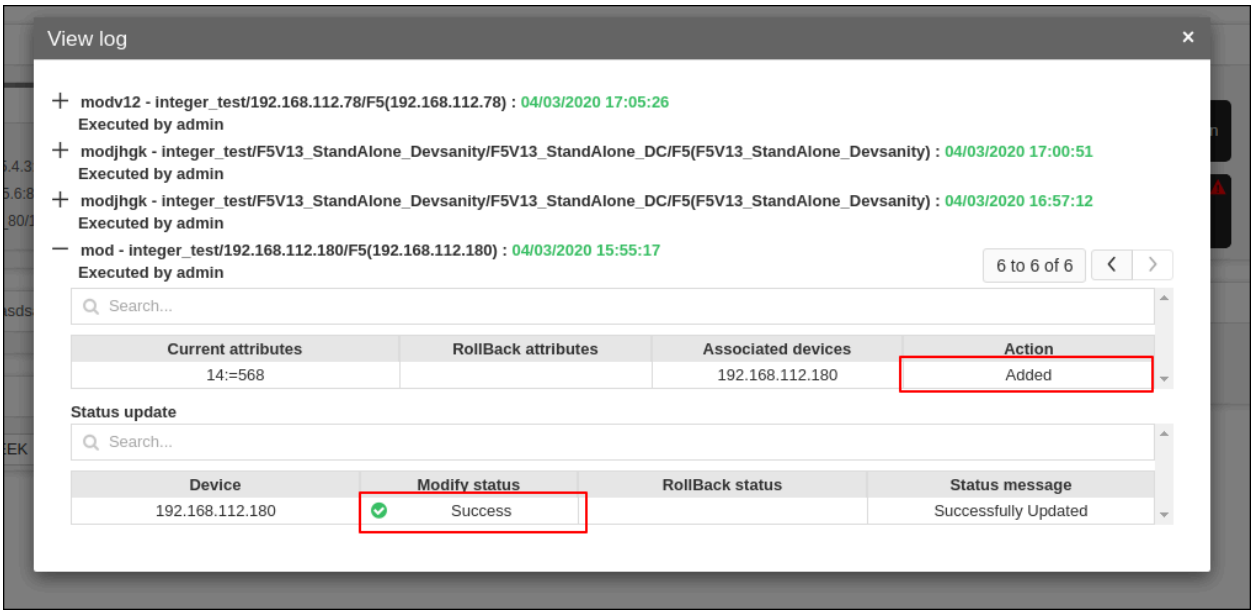


Modify Action Execution

1. Add/Modify the attributes and push it to Device Values.
2. Push the devices on which the action has to be executed.
3. Click **Execute**.

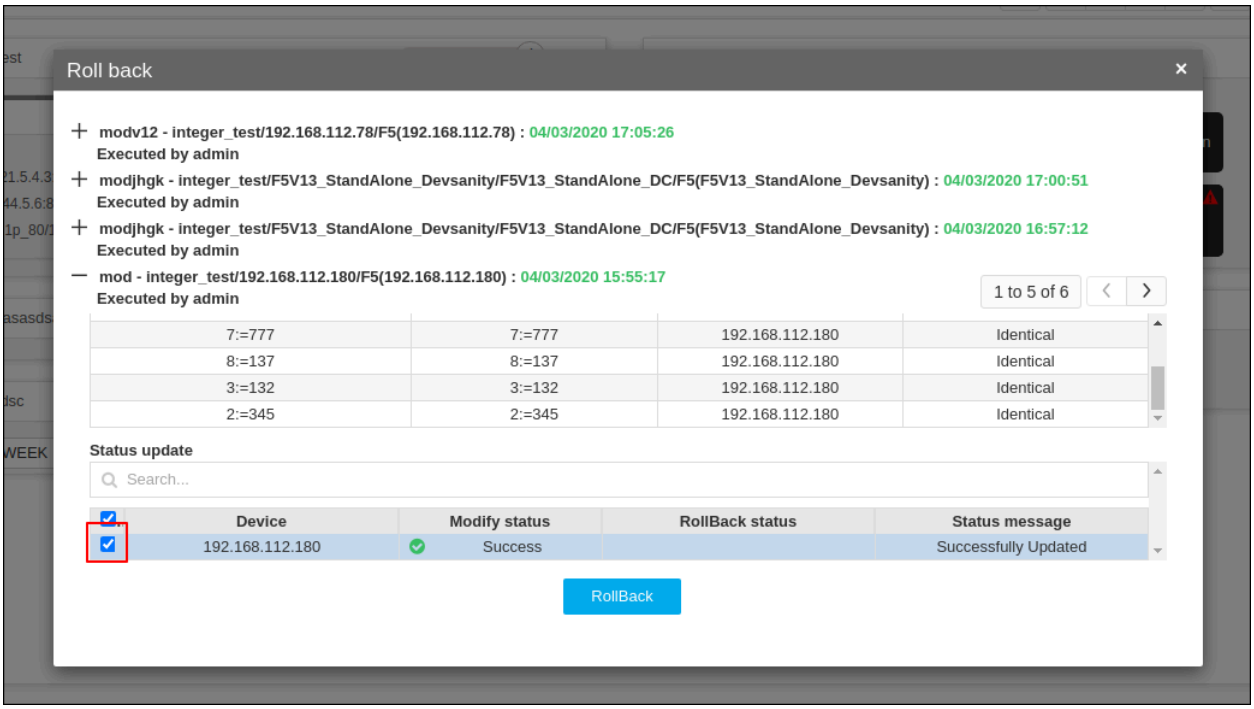
View Logs

For a particular group each Action Execution logs are maintained. Newly added attributes are easily identified. Action status is also updated. For any failure in action, the failure logs are updated in status message.



Rollback

The last action executed can be rolled back. Select the action and Click Rollback.



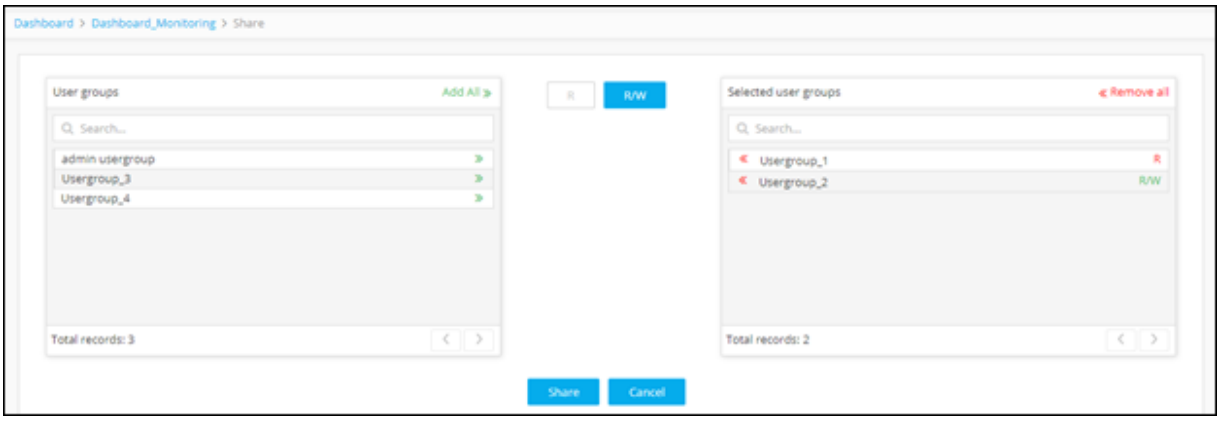
Dashboard Actions

Sharing a Dashboard

Based on your permissions, you may be able to share a dashboard.

To share a dashboard:

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If you have more than one dashboard, in the dashboard table, click the name of the one you want to share.
3. When the dashboard opens, click the (**Share**) button in the Command bar at the top of the screen. The Share screen appears.
4. Begin the assignment process by clicking the R (**Read-Only**) button. Each role you assign next will have read-only permissions within the dashboard.
5. In the Roles field, click the (**Assign item**) icon beside each role you want to share the dashboard with on a read-only basis.
6. Click the R/W (**Read-Write**) button. Each role you assign next will have read/write permissions within the dashboard.
7. In the Roles field, click the (**Assign item**) icon beside each role you want to share the dashboard with on a read/write basis.
8. Click the **Share** button to finish.



Delete a Dashboard

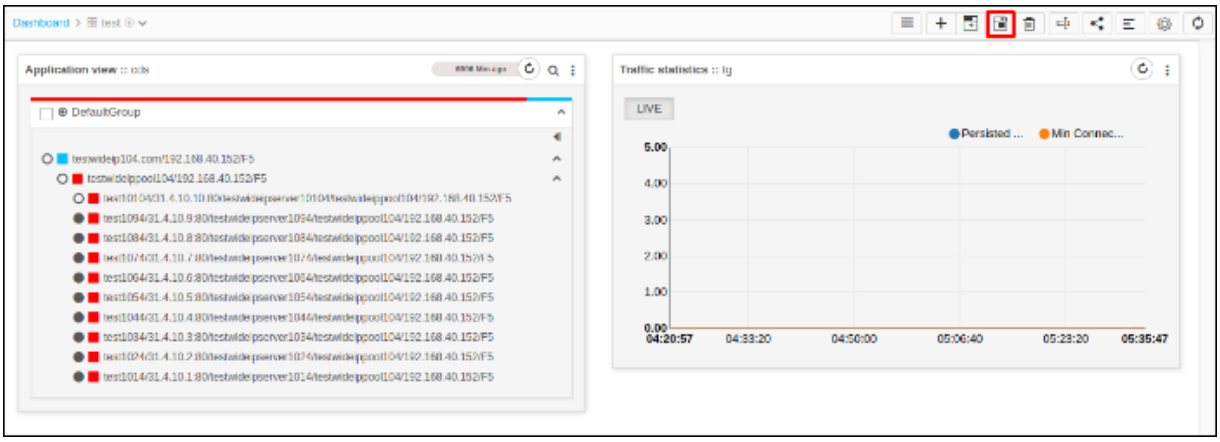
To delete a dashboard:

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If you have more than one dashboard, in the dashboard list, click the name of the one you want to delete.
3. When the dashboard opens, click the (**Delete**) button in the Command bar at the top of the screen. A screen pops up, warning you that deleting a dashboard also deletes all widgets on the dashboard.
4. Click **Yes** to continue.

Save a Widget

By default last created widgets will be displayed first in dashboards. This option can be used when the user wants to organize the widgets in the customized order.

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Menu** > **Dashboard**.
4. Go to any user defined dashboard.
5. Users can change the order of the widgets by drag and drop.
6. Click **Save Widgets.**



Rename a Dashboard

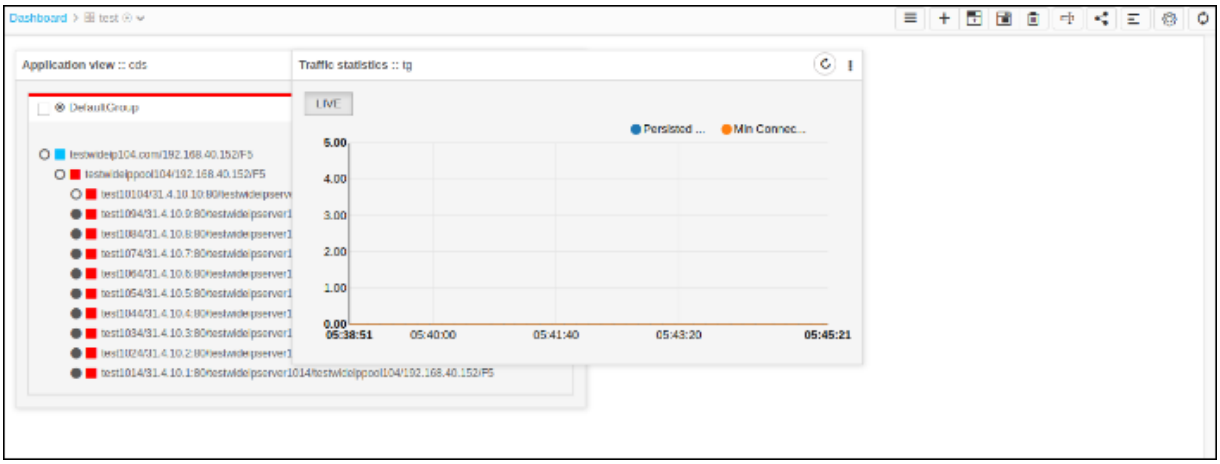
To rename a dashboard:

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If you have more than one dashboard, in the dashboard list, click the name of the one you want to rename.
3. When the dashboard opens, click the (**Rename dashboard**) button in the Command bar at the top of the screen.
4. On the Rename dashboard screen that pops up, enter a new name for the dashboard.
5. Click **Update** to finish.

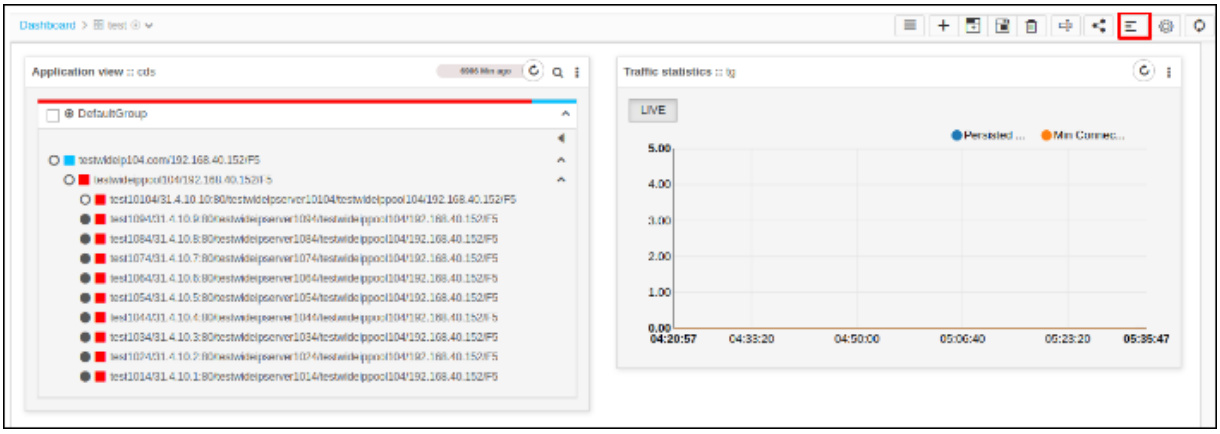
Align Widget

AppviewX gives an option to align the widgets if it gets misplaced.

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Menu** > **Dashboard**.
   Consider the widget in the dashboard is misplaced.

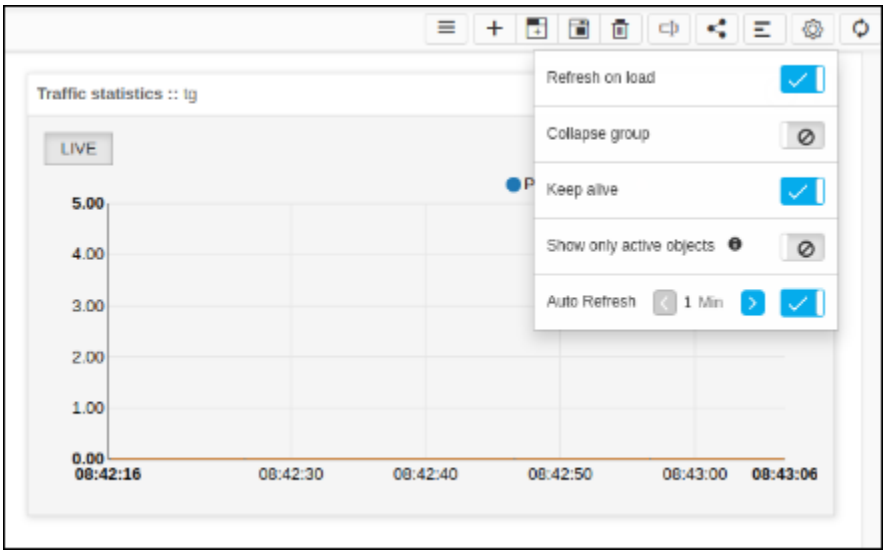


4. To align dashboards in their place click **Align**.

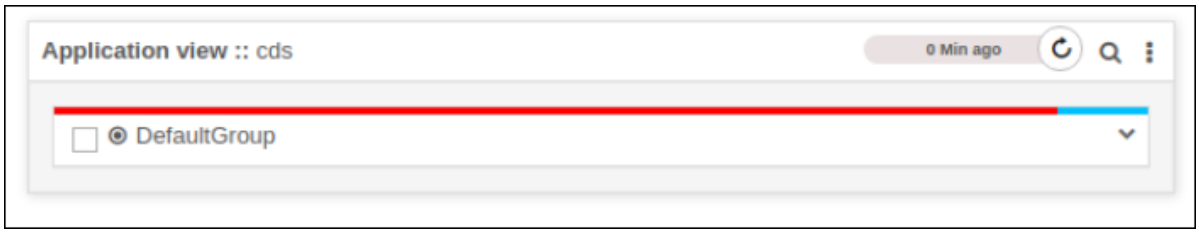


Settings

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **Menu** > **Dashboard**.
4. Click on the **Settings** icon.
5. Users can change the setting by clicking the corresponding slider.



- **Refresh on load** - If this setting is enabled, each time the dashboard loads, it will trigger the refresh call automatically to load the latest data.
- **Collapse group** - If this setting is enabled, all the groups inside the widgets on the dashboard will display in collapsed format by default.



- **Keep alive** - If this setting is enabled, the auto session expiry function will be disabled. Using this user can monitor the objects without session timeout interruptions.
- **Show only active** - If this setting is enabled, the objects of an active device alone be displayed from the configured objects. It is applicable only for **Application view widget**.
- **Auto refresh** - If this setting is enabled, dashboard refresh call will be triggered automatically in the given interval. Users can configure the auto refresh interval.

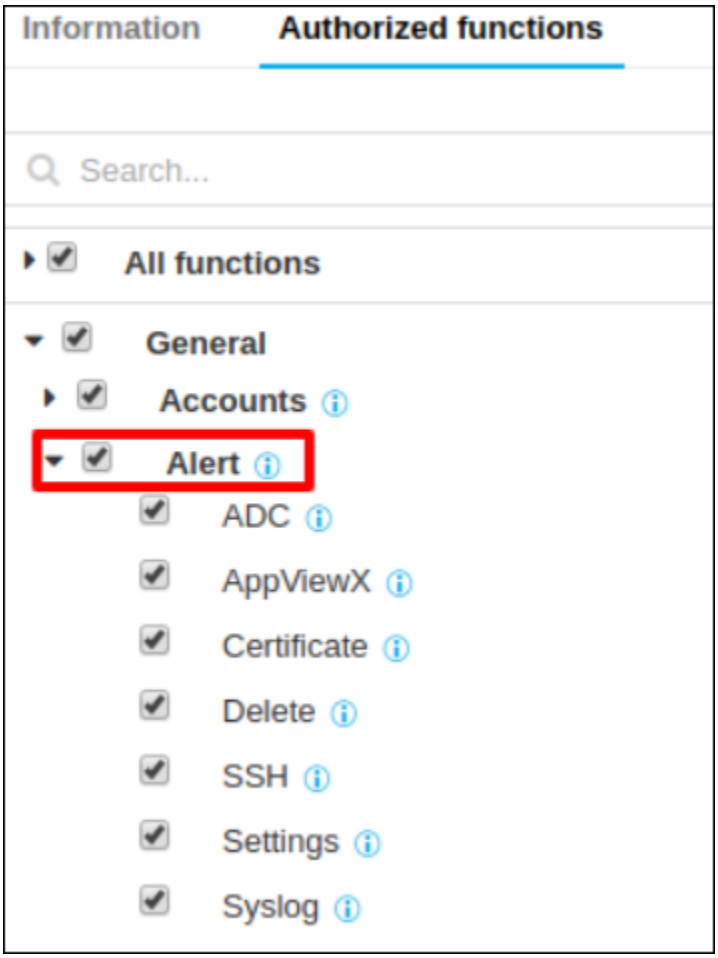
Alert Management

- Before you begin
- Create an ADC Alert
- Create a Syslog Alert

- Change alert settings
- Deleting alerts

Before you begin

To view / configure alerts, the users should have the ACF permissions.



Create an ADC Alert

To create an ADC alert,

1. Go to **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts**.
2. Click  (**Settings**) icon on the top.
3. On the **Settings** screen that opens, click the ADC tab if it is not already open.
4. In the **Alert name** box, enter a name for the alert.
5. In the **Alert message** field, enter the message that users will receive for the alert.

6. In the **Trigger** region, in the **Alert category** field, you can choose from **Threshold Alert**, **Application Alert**, and **Device Alert**.

> **Note:** Rather than adding objects manually, you can click the Add search string link and create a search string that automatically assigns all existing objects that match the filter criteria to the alert. The benefit of using a search string rather than selecting objects manually is that the search string continues to work in the background, auto-assigning all new objects to the alert if the objects match the search criteria you set up.

7. From the **Alert severity** dropdown list, select one of the following options:
   - **Critical** - For issues that are causing disastrous results or impacts on functionality. These are top priorities and must be resolved immediately.
   - **Fatal** - For issues that can cause disastrous results or impacts on functionality. These are a major priority and should be resolved soon.
   - **Major** - For issues that are important and require a resolution, but that is not the highest priority.
   - **Minor** - For issues that are of low priority and need a resolution.
   - **Notification** - For issues that are not alerts or warnings, but which must eventually be addressed.
8. In the **Vendor** field, select from the vendor whose device or devices you want to set an alert for.
9. In the **Object type** field, select the vendor object that you want to set an alert for. The contents of this field vary depending on the vendor you selected in the previous step.
10. In the **Available** field, click the » (**Assign**) icon beside each object/device you want to add to the alert. The following Alert conditions are applicable only for the Threshold alert.

> **Note:** To add another condition to the alert, click the (**Add**) button, then in the **Logic** field select **AND** or **OR** to define the relationship between the first condition and the second. AND relationships require both conditions to be met for an alert to be sent, OR relationships require that only one condition be met for an alert to be sent. Only based on the above user-defined conditions, threshold alerts will be raised in AppViewX.

- In the **Alert interval** field, select how often you want the system to check for breaches of the threshold levels that you are about to define. Checks can be set to occur every 10, 20, 30, 40, 50, or 60 seconds.
- In the Cool off the period field, select how much time the system should wait before sending another alert about a continuing threshold breach: 10, 20, or 30 minutes.
- In the **Statistics** field, define the conditions that will generate an alert by selecting values in the **Statistics**, **Operator**, and **Value fields**.

11. To send an email alert, **SMTP** must be configured. Refer to the Configure SMTP for Email Alerting topic for details on how to do this. When you have finished, complete the following steps to use email as an alert method:
    - Select the **Email Configuration** checkbox.
    - In the **Email Address** field, enter email addresses to send the alert. Use commas to separate the addresses.
    - In the **Subject** field, leave the default text or enter the text that briefly describes the kind of alert the user is receiving in their Inbox.
12. To use the **Simple Network Management Protocol (SNMP)** to send the alert, complete the following steps:
    - Enter the **Destination IP** for the alert.
    - Select the **Version** of SNMP you want to use: V1 or V2.
    - Enter the port of the alert that should be used for the alert.
    - Enter the **Community String** for the alert. The string is similar to a user ID or password and allows users to access the requested information on the device.
13. Click **Add** to save the alert to the AppViewX system.

Note: For the Application and Device alert, when any user executes changes on the configured application/device(s), AppViewX sends a notification based on the appropriate actions associated with the alert (Email/SNMP). Only the changes that are executed via AppViewX will be tracked and notified.

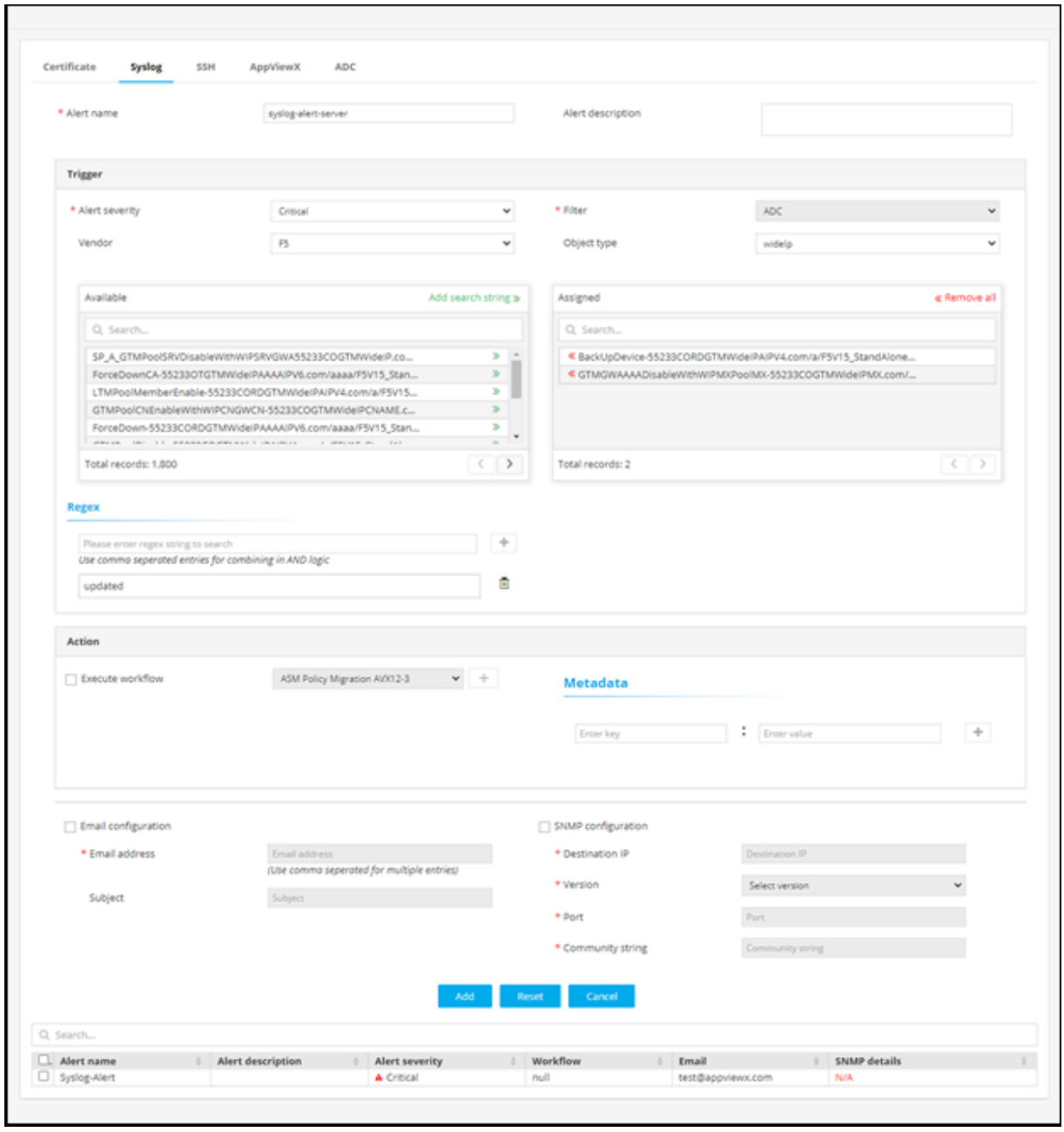
Create a Syslog Alert

AppViewX subscribes to all device-level logs, where it acts as a syslog listener. The logs of any

devices added in AppViewX can be viewed as syslog by navigating to Logging->Syslog. However, devices tend to generate huge amounts of data, a Syslog alert is a convenient way to get notified about a specific event that is of importance to you. It also allows for a closed loop remediation by associating workflows.

To create a syslog alert,

1. Go to **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts**.
2. Click on  (**Settings**) icon, and then **Syslog** tab.
3. Provide an **Alert Name** and **Message**.
4. Mention the **Severity**, it could be one or multiple.
5. Configure the critical Device/Applications that need to be monitored.



6. Add the Pattern/Regex that needs to be monitored on the Syslog received. Multiple strings can be provided with comma-separated, which will be considered as Boolean AND operator.
7. Following are some of the alerts that can be configured,

   • Sample syslog - <133>Sep 19 04:24:38 bigip-40-152 notice mcpd[6046]: 01070417:5: AUDIT - user admin - transaction #84153993-4 - object 0 - create { virtual_server_profile { virtual_server_profile_vs_name \"/Common/testVs\" virtual_server_profile_profile_name

\"/Common/tcp\" virtual_server_profile_profile_type 5 virtual_server_profile_profile_context 0 } } [Status=Command OK]\n

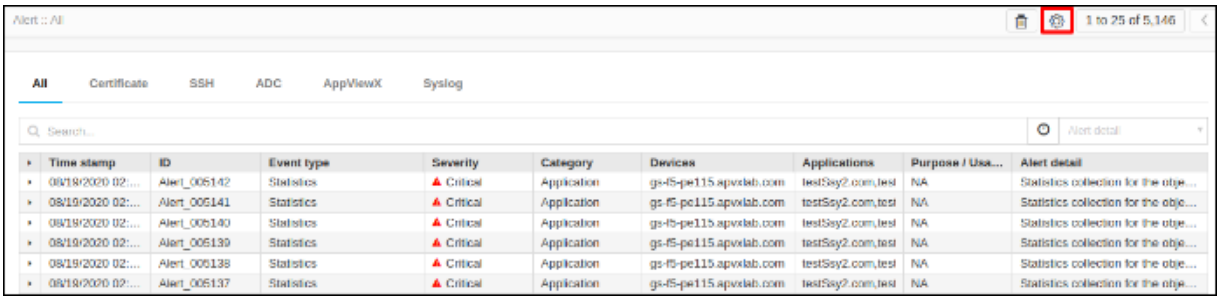
- For instance, if the Syslog alert is configured for the object and the Regex pattern is given as “create” Whenever an object is created and a Syslog is received for that object as above. An alert will be raised for the same and notified to the user.

8. You can also pass certain metadata from the alert to the workflow. In the Metadata section, enter a key and its associated value in the respective fields. This is the additional information that will be used by the workflow that is going to be associated with.
9. Associate any out of the box or custom workflow that needs to be executed on the occurrence of a configured Syslog event.
10. Configure multiple Alerts as needed and Add it to the Grid. The configured Alerts could be modified or deleted anytime by selecting the Alert from the grid.

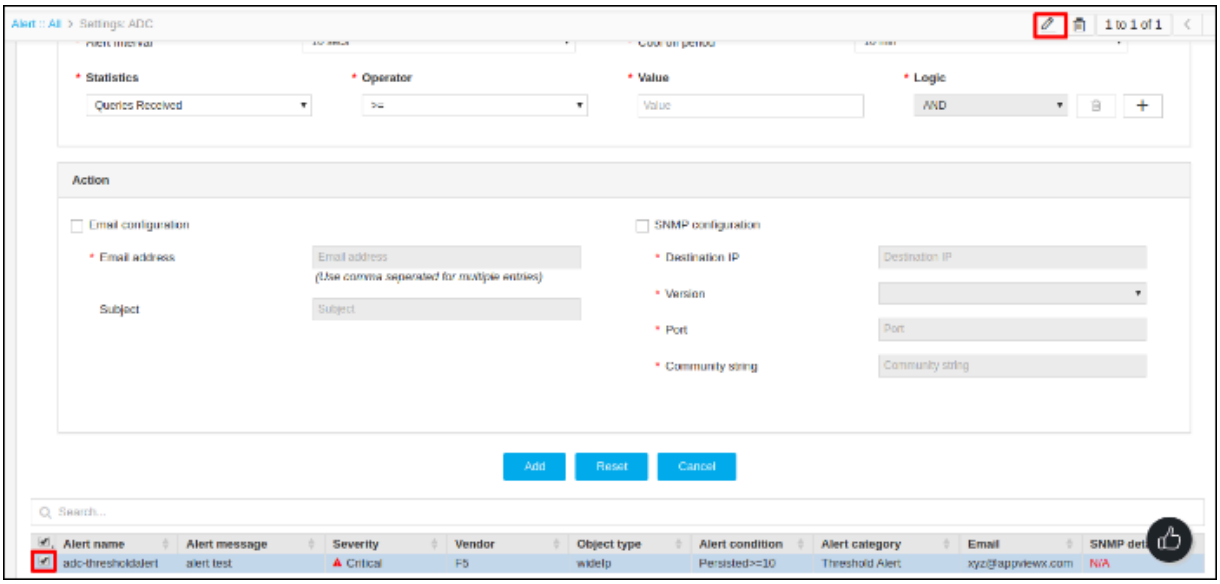
Change alert settings

Fields in alert settings may differ based on the alert type, but the process for modifying the alert settings is identical. To modify the alert settings use the below steps:

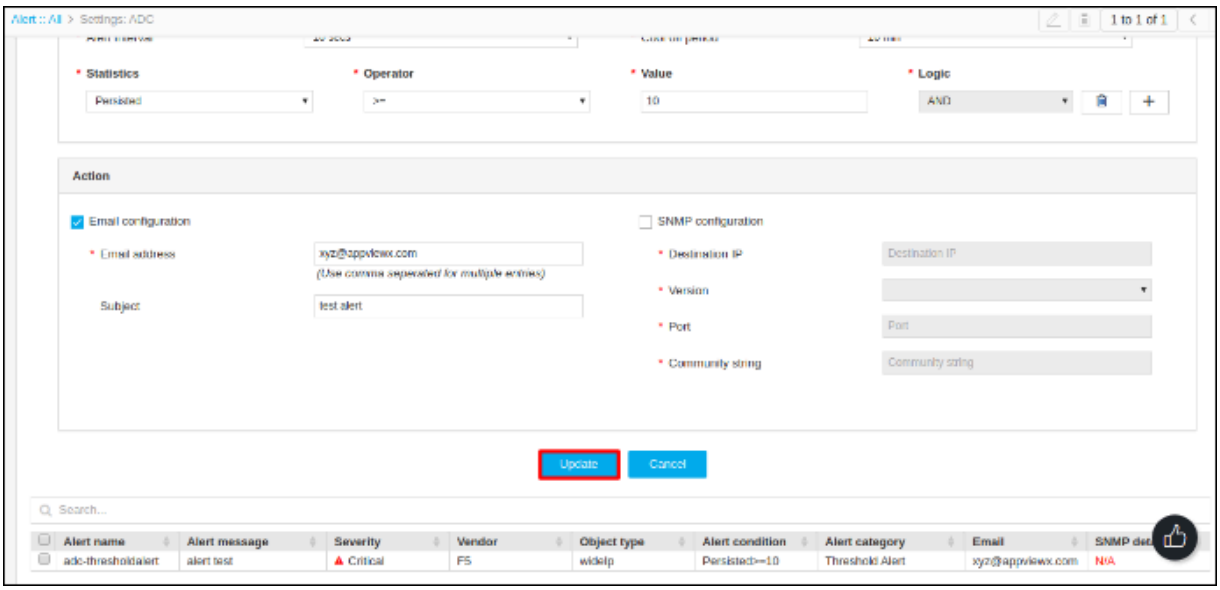
1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Alert**.
3. Click on the **Settings** button.



4. To modify the alert settings of a particular alert type click on the corresponding tab. For example ADC or Syslog.
5. Select an alert from the table and the modify button in the top right cornea will be enabled.
6. Click on the **Modify** button and make the required changes.



7. Click **Update**.

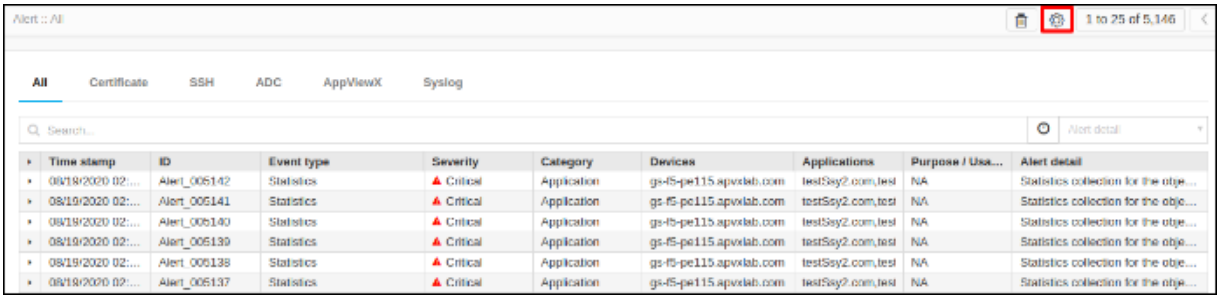


Deleting alerts

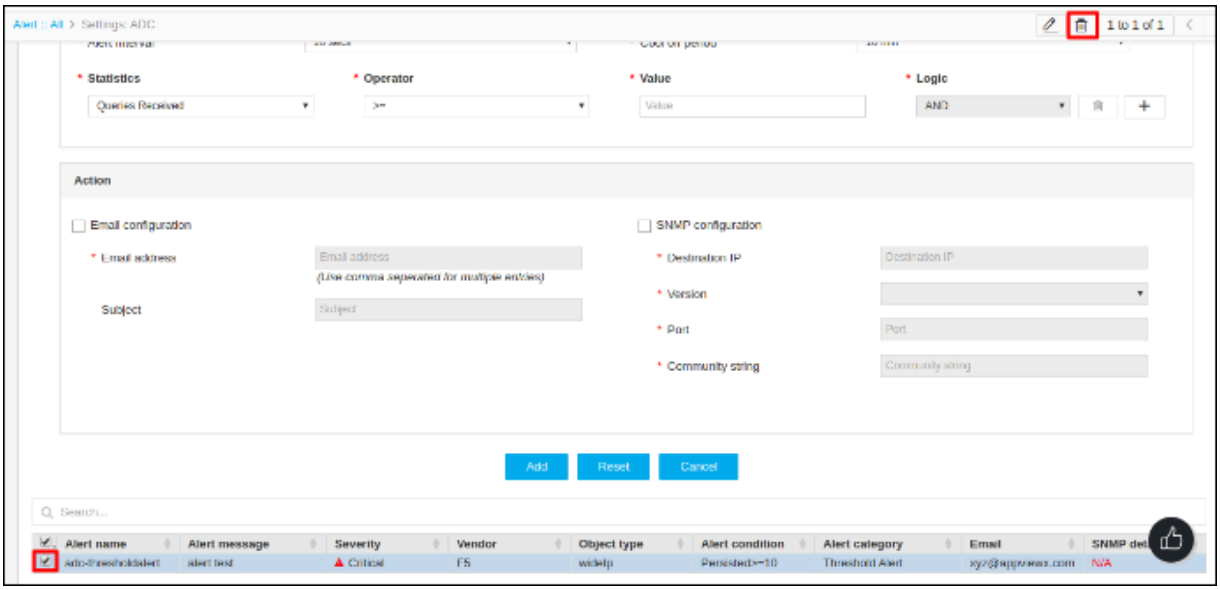
Fields in alert settings may differ based on the alert type, but the process for deleting the alert settings is identical. To delete the alert settings use the below steps:

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Alert**.

3. Click on the **Settings** button.



4. To delete the alert settings of a particular alert type click on the corresponding tab. For example ADC or Syslog.
5. Select an alert from the table and the delete button in the top right corner will be enabled.
6. Click **Delete**.



Chapter 9: System Settings

Device Settings

The device settings can be configured in the following tabs:

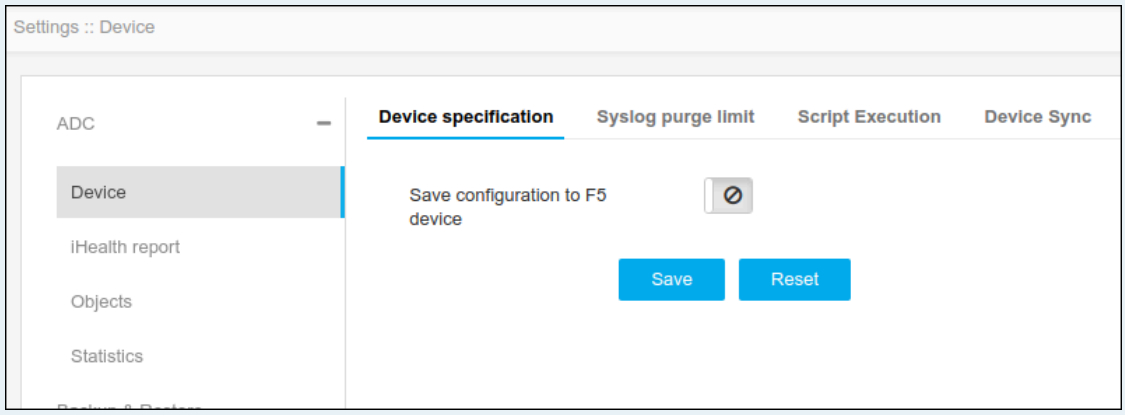
Configuring Device Specification

Save the changes of device specification configuration on the F5 device after config fetch. This enables all the changes to be reflected on the F5 file.

To configure a device specification,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Device** > **Device Specification** tab.
2. Click the toggle icon to enable Save Configuration to the device.

Note: In this example, F5 device specification is shown.



3. Click **Save**.

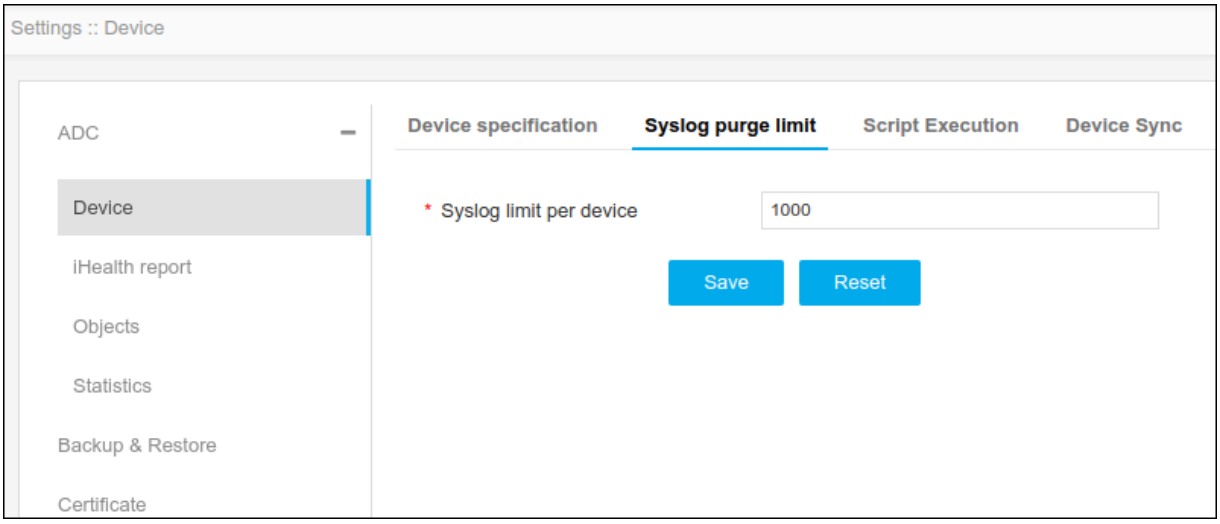
Note: To reset the changes, click Reset.

Configuring Syslog Purge Limit

Syslog purge limit enables to limit of the number of Syslog persisted against a device. The oldest logs will be automatically deleted on exceeding the limit.

To configure the Syslog purge limit,

1. Click **Menu** >**ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Device** > **Syslog purge limit** tab.
2. On the Syslog purge limit tab, specify the syslog limit per device. By default, the limit is set to 1000 and can be extended till 5000.



3. Click **Save**.

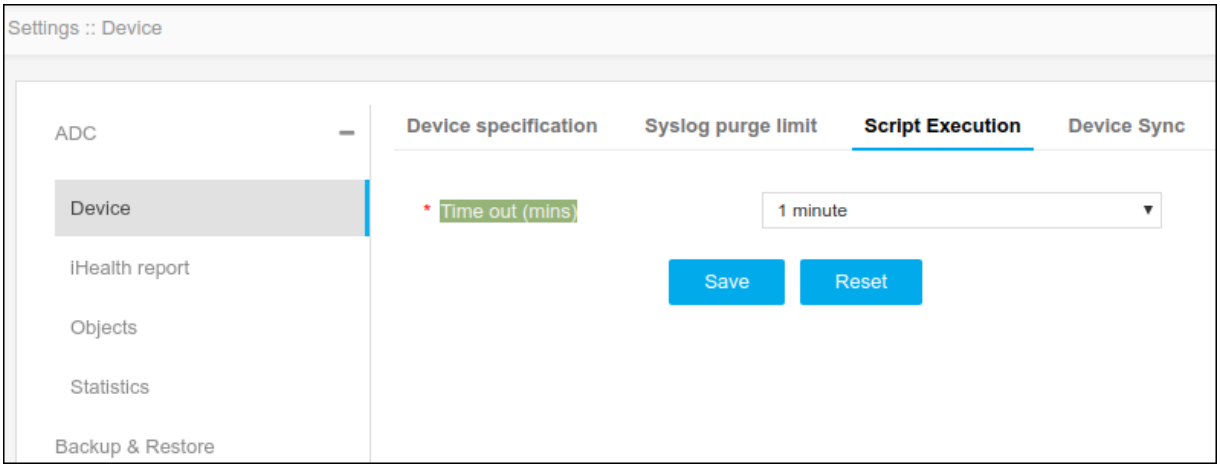
> **Note:** To reset the changes, click Reset.

Configuring Script Execution

Script Execution setting allows you to specify the time-out limit of script execution. If the script execution exceeds the specified time, AppViewX will automatically terminate the script.

To configure script execution,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Device** > **Script Execution** tab.
2. On the Script Execution tab, specify the timeout limit.



3. Click **Save**.

> **Note:** To reset the changes, click **Reset**.

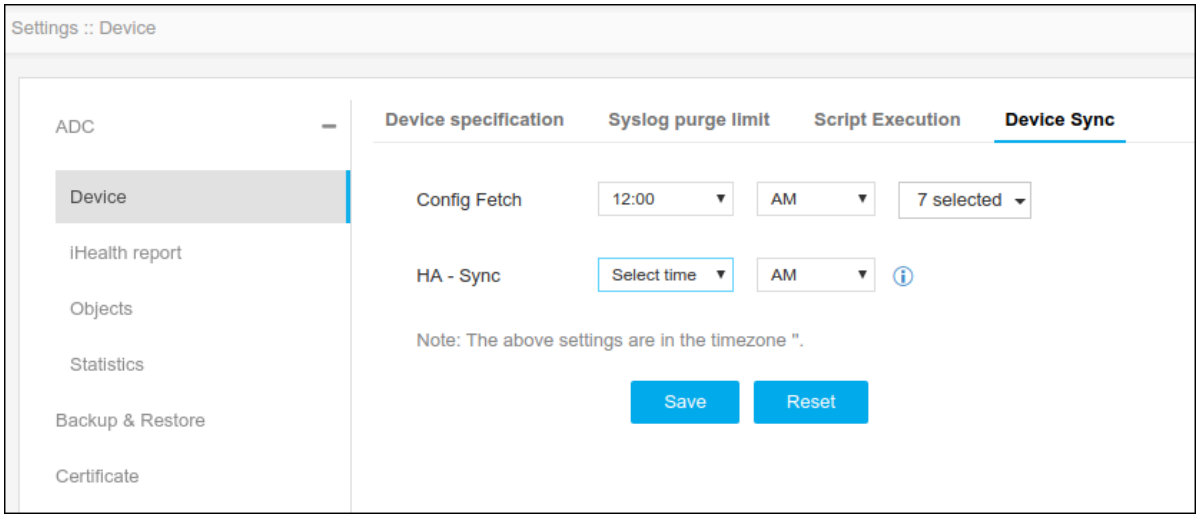
Configuring Device Sync

The device Sync feature allows to customize the configuration sync operations.

To customize the configuration sync operations,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Device** > **Device Sync** tab.
2. On the Device Sync tab, specify the following:
   - **Config fetch** - Allows to schedule the config fetch process at a specific time for selected days. Ensures device changes are reflected in AppViewX.
   - **HA - Sync** - Ensures the HA devices are synchronized in specified intervals.

     Note: To set device sync, the AppViewX Group Sync flag must be enabled while adding a device to run HA sync as per configured interval.



3. Click **Save**.

Note: To reset the changes, click **Reset**.

Object Settings

The object settings can be configured under the following tabs:

- Actions
- Naming Format
- Configuration drift

Configuring Action Settings

On the Actions tab, you can customize the actions execution as needed

To customize the actions,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Objects**.
   By default, the **Actions** tab appears.

2. Enable the **Make Comments Mandatory** toggle button to set the comments option mandatory while executing an action from the Control Center or dashboard. This ensures end users are mandated to mention the reason for their actions.
3. Enter comments in the **Comments Placeholder**, such as SNOW ID, Enter Application impacted, etc. to impose a standard to be followed upon action execution.
4. Select **Active**, **All Peer**, or **Specific Device** radio buttons for **Execute Action on Device**. By default, AppViewX actions are triggered on current Active devices. This can be modified as needed.
5. Ensure Peers are associated in AppViewX for seamless execution.
6. Click **Save**.

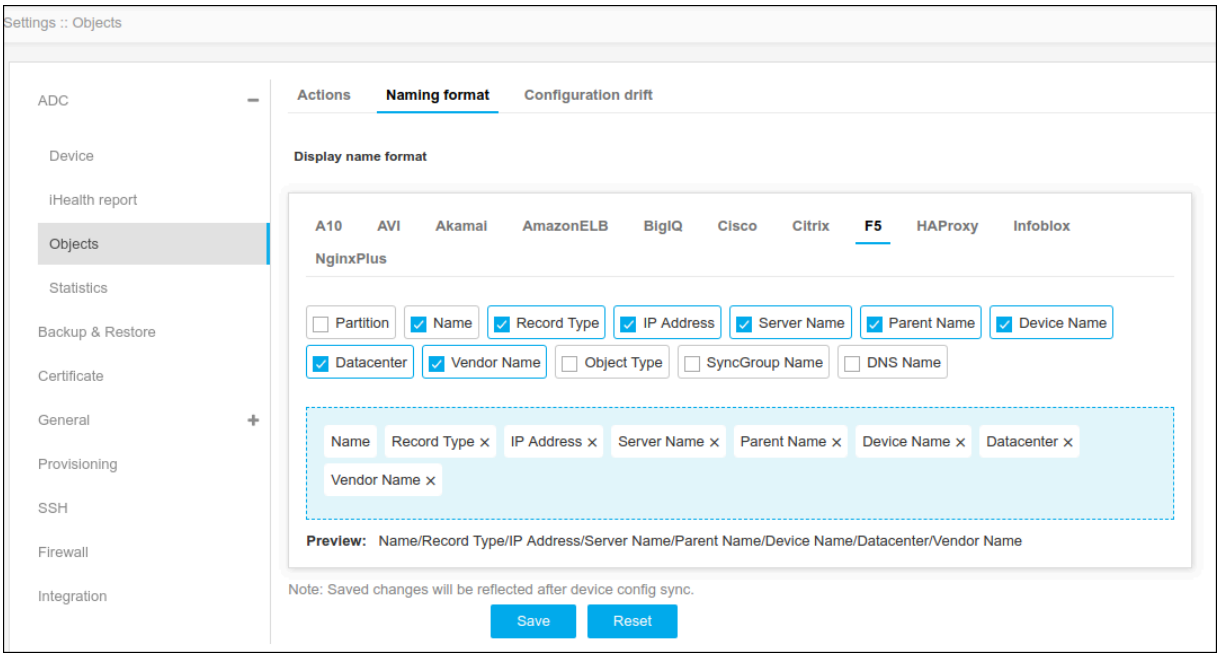
> **Note:** To discard the changes, click **Reset**.

Configuring Object Naming Format

On the Naming Format tab, you can customize the display name format of your objects that needs to be followed throughout the application.

To customize the naming format,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Objects**.
2. Click the **Naming Format** tab.



3. On the **Display Name Format** page, choose the vendor to be modified and select the respective Property, reorder the fields as needed.
4. Click **Save**.

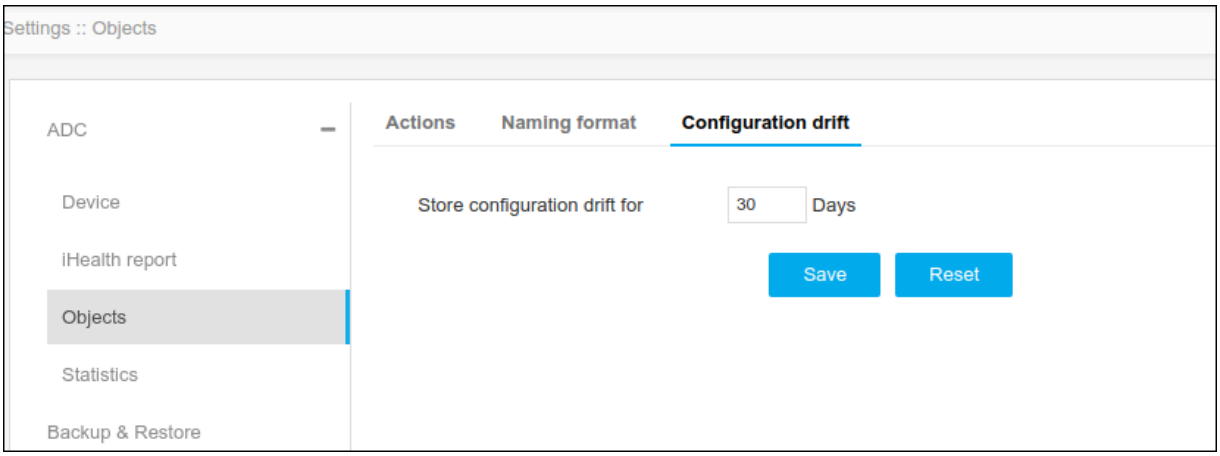
> **Note:** To discard the changes, click **Reset**.

Configuration Drift Storage Limit

AppViewX identifies the object configuration changes (as part of config fetch, Syslog notification, etc.,) and stores the drift to generate reports, governance, and rollbacks. You can customize the number of days the drift must be persisted.

To customize the number of days for the configuration drift,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Objects**.
2. Click the **Configuration Drift** tab.



3. Enter the store configuration drift value up till 90 days in the Store Configuration Drift for the field.
4. Click **Save**.

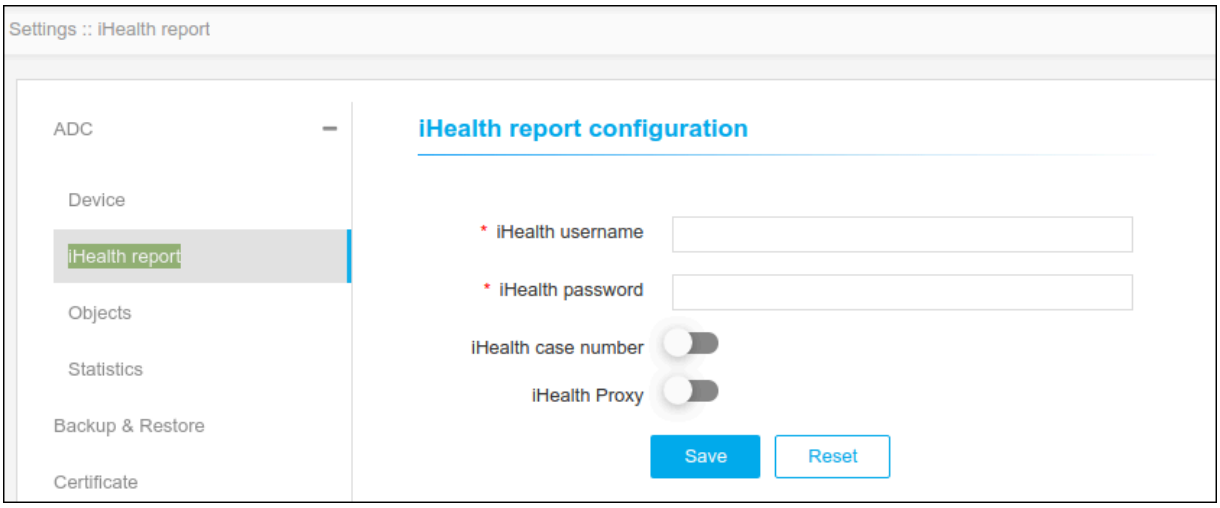
Note: To discard the changes, click Reset.

Configuring F5 iHealth Report Settings

Users can configure the F5 iHealth related setting on this page. iHealth is the feature in F5 used to diagnose health of the F5 device. In AppViewX, we collect the qkview file from the F5 device, push to the iHealth site and generate an iHealth report and that will be shown in the device inventory page under the iHealth report column. On this page, users can configure the username and password to be used for logging into iHealth site. In addition to that, users can also enable/disable whether proxy is to be used for iHealth login and whether a case number is mandatory for iHealth report

To configure the iHealth report,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **iHealth Report**.



2. On the **iHealth Report Configuration** page, enter the **iHealth username** and **password**.
3. Enable the **iHealth case number** and **iHealth Proxy** toggle buttons to upload the generated qkview file against the mentioned case number for future reference.
4. Click **Save**.

Note: To discard the changes, click **Reset**.

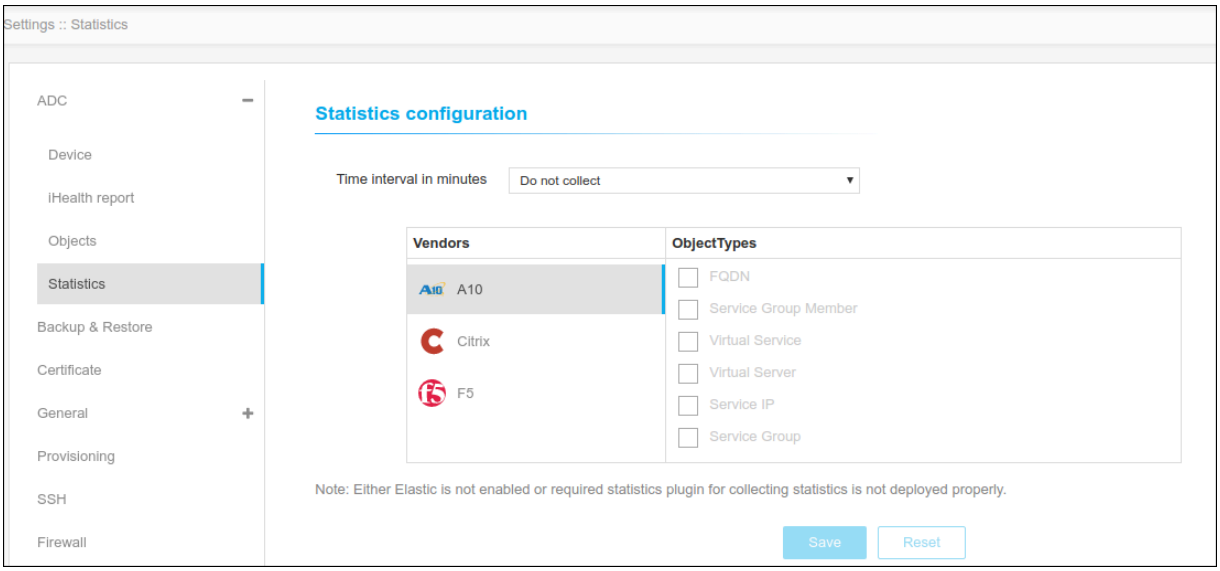
Configuring Statistics Collection

In the statistics module, AppViewX collects the statistics of the LTM and GTM objects. It used to monitor the Load and performance of LTM and GTM Objects and devices. Users configure types of objects that need to collect statistics and time intervals at which statistics need to collect.

- Configures the statistics data collection to monitor the historic statistics with respect to the vendors and object types.
- Statistics plugin has to be deployed in the node for collecting statistics data.
- AppViewX will collect the stats, aggregate them and provide out of the box reports in the form of dashboards.

To configure statistics,

1. Click **Menu** > **ADC+** > **SETTINGS** > **Module Settings** > **ADC** > **Statistics**.



2. On the **Statistics Configuration** details page, choose the time from the **Time Interval in Minutes** drop-down.
3. Select the vendor, and then choose the object types and devices from the list for which statistics must be fetched.
4. For the device selection, click the **DEVICES** tab, and then,
   - Select the **Type** of device selection as **Device** or **Device Groups**.
   - When you select the **Device** radio button, you get the option to select the devices from the list either by searching or using regex.

     Note: If Regex is added for filtering the device, the statistics will be configured for the newly added devices as well, which match the regex.

   - When you select the **Device Groups** radio button, you get the option to select the device groups from the list.

5. Select the default view for the Traffic statistics widget from the **Default View** dropdown. The possible options for default view are:

- Day (default)
- Live
- Week
- Month
- Quater

6. Click **Save**.
   AppViewX collects the stats, aggregates them, and provides out-of-the-box reports in the form of dashboards.

Note: To discard the changes, click **Reset**.

Chapter 10: Schedulers Used by ADC+

By deployment, the scheduler below will be activated for ADC specific functionality monitoring purposes. On demand these schedulers can be modified with the help of a support team

Scheduler Name	Description	Frequency
AdcBackUpDeviceJob	BackUpDeviceJob for Adc	Every 30 Minutes
AdcDownloadConfigJob	DownloadConfigJob for Adc	Every day at 00:00:00 AM
AdcDeviceSyncJob	Device sync Job for Adc	Every 15 Minutes
AdcDNSReverseLookupJob	Dns reverse lookup Job for Adc	Every day 6AM & 6PM
SyslogPushJob	Syslog Push for Subsystems	Every 5 Minutes
SyslogCDUJob	Syslog CDU Trigger	Every 1 Minutes
StatAggregationJob	Statistics Aggregation Job.	Every 6 Hrs Start from 00:00:00 Hrs
PurgeRawStatisticsJob	Purge Raw Statistics Job	Every day at 1 AM
PurgeAggregateStatisticsJob	Purge Aggregate Statistics Job	At 01:00:00am, on the 1st day, every month starting in January
UnusedObjectsReportAggregationJob	Unused Objects Report Aggregation Job	Every day at 00:30:00 AM
ADCDashboardStatisticsCollect	Statistics collection for Heatmap and traffic statistics widget	Every 5 seconds
AdcConfigFetchValidatorJob	Validate ConfigJob for Adc in given Interval	Every 15 Minutes
ADCConfigDriftPurgeJob	Purge job for config drift logs	Every day at 00:00:00 AM
ADCVipTrafficAggregator	Aggregator job for calculating total traffic served	Every 1 hour
ADCVipTrafficAggregator	Aggregator job for calculating total traffic served	Every day at 00:00:00 AM

Scheduler Name	Description	Frequency
ADCApplicationTrafficHourAggregator	Aggregator job for calculating total traffic served by an application	Every 1 hour
ADCApplicationTrafficDayAggregator	Aggregator job for calculating total traffic served by an application	Every day at 00:00:00 AM
AVRLogsProcessingJob	Aggregator job for calculating top talkers to VIP	Every 15 Minutes
PurgeAvrLogsJob	Purge job for top talkers to VIP	At 01:00:00am, on the 1st day, every month starting in January
AdcDeviceHASyncConfigurableJob	Device ha sync configurable Job for Adc	Every day at 10:00:00 PM
AdcBackUpDeviceMonitorJob	Monitor BackUpDeviceJob Scheduler for Adc	Every day at 11:45:00 PM
ADCStateStatusDriftPersist	Persist adc object state status drift	Every day at 03:00:00 AM
ADCStateStatusDriftPurge	Purge adc object state status drift	Every Sunday at 03:00:00 PM