appviewX

ADC+ User Guide

Version: 2020.3.0

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 2020.3.0	September 2020

About the Documentation

This guide explains the capabilities of AppViewX's multi-vendor Application Delivery Controller (ADC) platform and provides step-by-step instructions to manage, automate, orchestrate, and monitor the application delivery services.

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

- ADC Overview
- Types of ADC/Load Balancer
- Need for Centralised ADC Service Lifecycle Management Console/Interface etc.
- About AppViewX
- AppViewX ADC+ Introduction
- Accessing the ADC

ADC Overview

Application Delivery Controllers (ADC)/Load balancer distributes network traffic across servers. It acts as a reverse proxy to increase the reliability of the applications by distributing incoming traffic from clients across multiple server resources.

Three core functions of load balancers are:

- Efficiently distribute Network Load or Client's Request across servers.
- Sending requests to the server available, enabling high application availability.
- Increase and decrease the number of servers based on traffic.

Types of ADC/Load Balancer

On a high level, there are 3 types of Load Balancer based on appliance:

- Hardware-based Load Balancer
- Cloud-Based Load Balancer
- Software-based Load Balancer

Hardware-based Load Balancer

A Hardware-based load balancer typically has a dedicated hardware appliance with relevant features. These are expensive to purchase and maintain, but gives users the full control and comes in different hardware configuration based on traffic requirement.

Popular hardware-based load balancer :

- F5
- Citrix Netscaler
- A10

Cloud-Based Load Balancer

A Cloud-Based Load Balancer is available on the cloud with full features, without the headache of purchasing and maintaining the costly hardware. It gives the user the option of "Pay as you use".

Popular cloud-based load balancer:

- Amazon Web Services (AWS)
- Google Cloud (GC)
- Microsoft Azure

Software-based Load Balancer

A software-based load balancer id is available as a code. It can be installed on the server to turn them into load balancers. It also gives you the flexibility of choosing your own platforms like Windows, Linux, or Docker.

Popular software-based load balancer:

- HAProxy
- Nginx
- AVI

Need for Centralised ADC Service Lifecycle Management Console/Interface etc.

The Growth of IT Infrastructure is directly proportional to the growth of Business. As the IT Infrastructure grows it eventually includes the need for load balancers from many different vendors. The decision to include multiple vendors might be the relic of time, cost, and requirement of a specific application. Managing and maintaining it requires lots of resources and a comprehensive long-term plan.

The advantage of having diverse load balancer vendors is, your entire infrastructure is not vulnerable to specific network attacks or viruses. The disadvantage is managing different vendor products requires complex and costly support. Most of the time various product services come with different management tools, making IT infrastructure management complicated and unorganized.

AppViewX is Set to change all that, It is a modular, low-code software application that enables the automation and orchestration of network infrastructure using an intuitive, context-aware, visual workflow. It is closed-loop and state-aware, capable of verifying that intent has been achieved and providing actionable insights and automated remediation.

About AppViewX

The AppViewX Platform is the industry's first product category that offers Multi-vendor load balancer-centric Management, Automate and Orchestrate best-in-class and open-source application delivery services, and enables Self Servicing capabilities. It supports both traditional and non-traditional ADCs from leading vendors - A10 Networks, Akamai Technologies, Amazon Web Services (Elastic Load Balancers), Brocade, Cisco, Citrix, F5 Networks, HA Proxy, NGINX, Radware.

AppViewX ADC+ Introduction

AppViewX enables NetOps & SecOps teams to support ever-increasing business demands with greater agility. It offers state-of-the-art management capabilities that map to the needs of application owners, network engineers, and network operations.

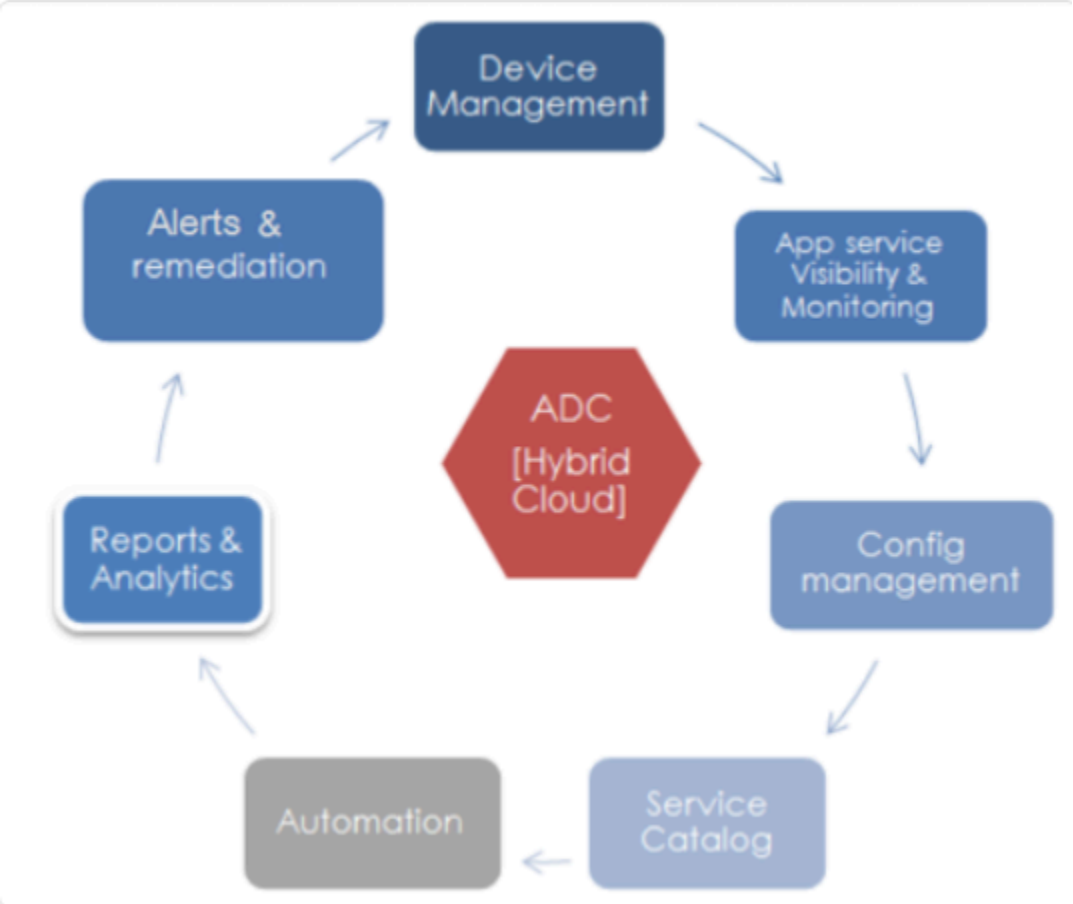
ADC is an intuitive platform for Management, Automation, Orchestration, and Observability for application delivery services across Hybrid multi-cloud environments. With ADC+, you can gain application-centric insights, visibility into application services, and simplify application delivery infrastructure operations. It offers a single pane of glass/Interface and a holistic view of your application delivery across hybrid multi-cloud environments.

- ADC Lifecycle Management
- Device Management
- App Service Visibility and Monitoring
- Configuration Management
- Service Catalog
- Automation
- Alert and Remediate

ADC Lifecycle Management

Lifecycle overview

The ADC lifecycle defines the processes by which a Device or an Application is Discovered, Managed, Monitored, Automated, and Remediated. The multi-vendor (Cloud, On-prem) and intent-based load balancer application lifecycle management solution continuously aligns itself to required service levels, security, and compliance policies.



Device Management

- AppViewX's centralized multi-vendor Inventory Management allows you to onboard the supported ADC vendor devices (Hardware, Cloud, and Software) into the AppViewX inventory using the IP Address/ FQDN.
- AppViewX will initiate communication using the provided credentials and Discover the Applications/ Objects along with their configuration that is hosted on the devices. The Discovered Applications can be accessed within the product.

- Access to each device and its application objects can be controlled using access control policies. The AppViewX Platform applies granular access control to application objects, certificates, and configuration templates.
- The solution makes it easy to control access and delegate tasks and integrates with external directory service systems such as AD, RADIUS, TACACS, and LDAP. Roles can be easily created, changed, or discontinued per the needs of the organization.

To know more, refer to the Device Inventory section.

App Service Visibility and Monitoring

- ADC provides App-centric visibility for your ADC infrastructure in a single window.
- The Search engine allows you to look for any application and recreates the topological view starting from the Global load balancer to the end server. This provides the network team visibility into the infrastructure to troubleshoot application-related issues faster.
- Get better insights into your Application health, state, status, utilization, and performance through pre-built dashboards. Monitor and Manage Application Traffic through Custom Dashboards and Widgets that allow Traffic routing, Monitor live traffic, and Distributes traffic ratio across data centers.
- Enables self-servicing and launch automation from application-centric views.

To know more, refer to the Dashboar section and App Search section.

Configuration Management

- Manage your network configuration by automating the backups, track and report network changes and ensure they are compliant with the defined policies.
- Audit the configuration drift and prevent unauthorized or unwanted changes by comparing the configuration across devices visually and restore the changes to adhere to the standards.

To know more, refer to the Configuration Management section.

Service Catalog

- ADC offers an intuitive self-service catalog to access service offerings for Line of Business (LOB), employees, and partners via customized pages.
- ADC ships out-of-the-box self-service catalog pages by persona for NetOps, Application Teams, SecOps based on the permissions assigned.

To know more, refer to Pages User Guide.

Automation

- AppViewX's Application Delivery Automation solution abstracts application infrastructure and business applications to automate changes on your ADC infrastructure.
- The Visual Workflow tool provides an intuitive system for designing self-serviceable, event-driven and intelligent automation workflows. It leverages best-in-class automation and orchestration methodologies to ensure faster application deployments in brownfield and greenfield environments.
- It offers prepackaged automation workflows to provision application delivery and Infra and error-free application deployment and orchestration.

To know more, refer to the Automation section.

Alert and Remediate

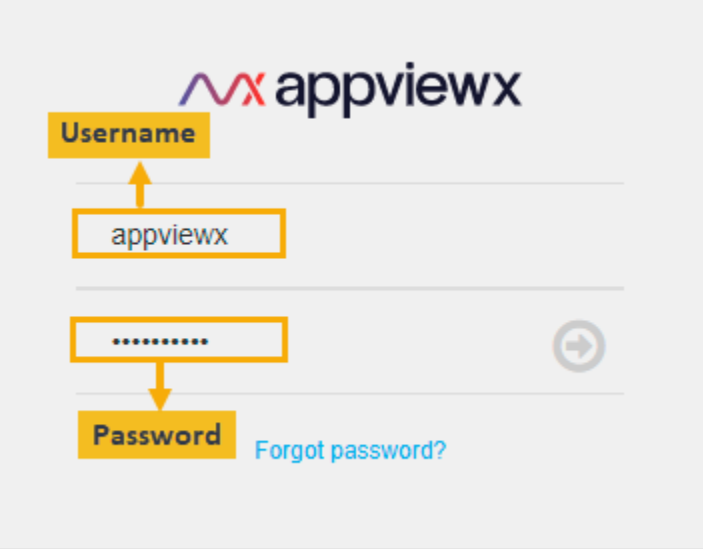
- Track all the activities that take place within AppViewX or any external entity that is connected to the AppViewX system in the form of logs and alerts.
- Periodically monitor your Application Services or Devices to get notified and automate remediation in the event of any critical changes.

To know more, refer to the Alerts & Logs section.

Accessing the ADC

Steps to access the ADC,

1. Log in to AppViewX with a valid credential (URL provided by AppViewX).



   The AppViewX Landing page appears.
2. Click the menu button located in the upper left corner of the screen.
3. Click **ADC+** on the left navigation bar.

Chapter 2: TRAFFIC MANAGEMENT

Dashboard Overview

AppViewX Platform helps Enterprise IT manage, automate, and orchestrate application delivery services providing an application-centric view into the state of the application delivery infrastructure running in multi-cloud environments. Application, network and security engineers may self-service and initiate automation workflows in a single click that deliver compliance and true business agility. This gives application and operation teams a topology view of the application delivery infrastructure with better insights into application health, state, status, utilization, and performance.

The Dashboard module enables the user to manage, monitor, and interpret all the configured applications and their objects. It uses customizable widgets for managing ADC objects. The dashboard comes with a variety of pre-made dashboard widgets (components) that you can use to build a specific dashboard view that meets the different needs of your business.

It has been categorized into Default Dashboard and Custom Dashboard.

- Change the Settings for a Dashboard
- Create a Dashboard
- Delete a Dashboard
- Export a Dashboard
- Import a Dashboard
- Rename a Dashboard
- Save the Dashboard
- Search for a Dashboard, Object, or Widget

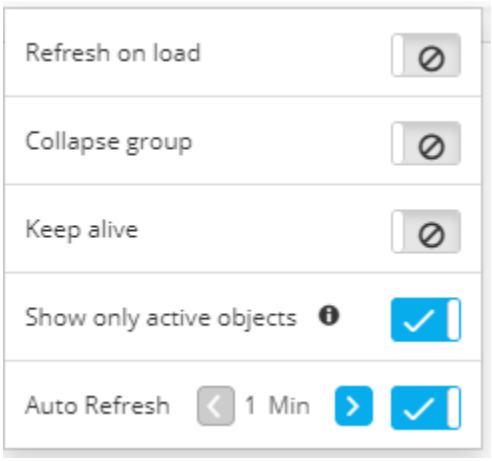
- Share a Dashboard
- Switch Between Dashboards

Change the Settings for a Dashboard

- AppViewX recommends to enable Syslog based configuration update so that any changes on the end devices with regards to state/status will be reflected in AppViewX on a near real-time basis ensuring a seamless experience.
- The ‘Last Refresh time’ on the widget displays the last time the widget is updated with the latest State/ Status information.
- Click on the ‘Refresh’ button on the widget to perform on-demand State/Status information. Each Object will contain a last refresh time on the tooltip, you can also trigger a refresh for a particular object from the tooltip.
- Enable ‘Auto refresh’ from the ⚙ (**Settings**) of the dashboard page with a particular interval (1 - 5 mins) which will automatically refresh the state/status information of the objects.
- Enable ‘Refresh on load’ from the ⚙ (**Settings**) of the dashboard page to get the latest state/status information on loading the dashboard.
- ‘Keep Alive’ option on the dashboard **Settings** ⚙ if enabled will ensure the session is not timeout by refreshing the dashboard every 15 mins.

To change the settings for 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 whose settings you want to view and/or update.
3. In the Command bar for the dashboard, click the ⚙ (**Settings**) button.
4. A dropdown menu appears, listing the settings you can change:



- **Refresh on load** - If this setting is enabled, each time the dashboard loads, it displays the latest data in the system.
- **Collapse group** - If this setting is enabled, each time the dashboard loads, all groups within widgets on the dashboard display in a collapsed state by default.
- **Keep alive** - If this setting is enabled, the dashboard expiry function is disabled, allowing users to monitor all objects on the dashboard without interruptions caused by session timeouts.
- **Show only active** - If this setting is enabled, the objects of an active device are displayed in run time. This functionality is applicable only for Application View widgets.

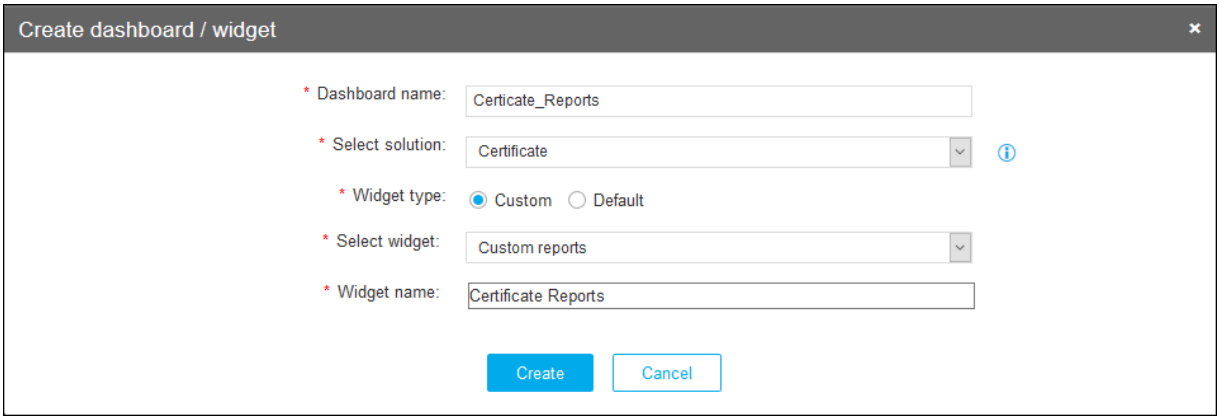
5. If the setting is currently disabled, a (**Disabled**) button appears.
6. If the setting is currently enabled, an (**Enabled**) button appears.
7. To change a setting, click the corresponding button and the opposite setting appears.

Create a Dashboard

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.

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.

Export a Dashboard

To export a dashboard from AppViewX,

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. Go to the top-level of the Dashboard module by clicking the Dashboard link in the breadcrumb field or click the  (**Dashboard inventory**) button in the Command bar.
3. In the dashboard table, select the checkbox beside the dashboard you want to export.

4. Click the (**Export**) button in the Command bar at the top of the screen.
5. On the Export Dashboard screen that pops up, select one of the following radio buttons:
   - **Report (.csv)** - Select this option if you want to view the dashboard as a CSV file and do not plan to import it into another build of the AppViewX platform.
   - **Import dashboard (.json)** - Select this option if you are downloading the dashboard with the intention of importing it into another build of the AppViewX platform.
6. Click **Export** to export the dashboard.

Import a Dashboard

To import a dashboard, the contents must be zipped and must contain single checksum .text files and/or .json files. This functionality is applicable only for the Dashboard that contains the Application View widget.

To import a dashboard into AppViewX,

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. Go to the top-level of the Dashboard module by clicking the Dashboard link in the breadcrumb field or click the (**Dashboard inventory)** button in the Command bar..
3. Click the (**Import**) button in the Command bar at the top of the screen. The Import screen appears.
4. Click the **Browse** button and then locate and select the zip file you are importing.
5. Click **Upload**.
6. The import function then checks to make sure the imported file and filename are valid.

After the zip file is successfully uploaded, select the checkbox in the column beside the dashboard name.

Note: If the dashboard has the same name as an existing dashboard, use the Dashboard name field on the Import screen to enter a new name for the dashboard you are importing.

7. Click the **Submit** button.
8. On the Confirmation screen that appears, click **Proceed**.
9. Click the Dashboard link in the breadcrumb field to return to the top-level *Dashboard* screen. The new dashboard appears in the list.

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.

Save the Dashboard

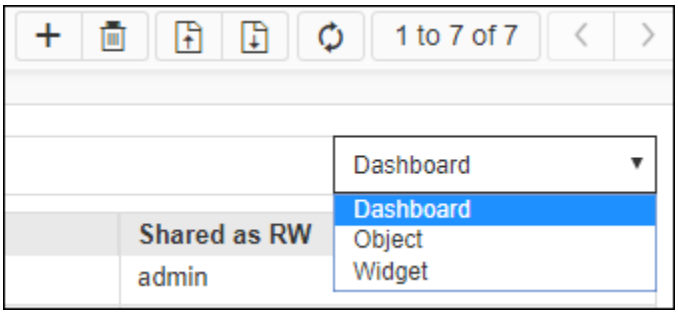
When you drag and drop the widgets to organize them in the dashboard, complete the following steps to save the changes:

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. After making necessary changes in the dashboard, click the  (**Save Dashboard**) button in the Command bar.
3. A pop-up message appears at the top of the dashboard, "**Dashboard saved successfully**."

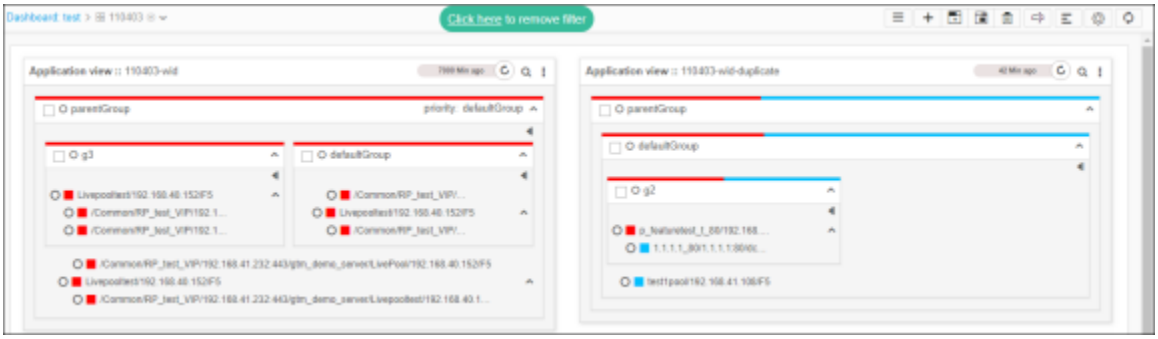
Search for a Dashboard, Object, or Widget

To search for a dashboard, object, or widget from the Dashboard screen,

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. Click **Dashboard** in the breadcrumbs trails at the top of the screen to go to the top-level Dashboard screen or click the **menu** button in the Command bar.
3. On the Dashboard screen that appears, enter the word or phrase you want to search by in the Search field.
4. Click the dropdown list at the right of the Search field and select the one you want to search for: Dashboard, Object, or Widget.



5. Click Enter on your keyboard to run the search. The results appear in a table below the search field.
6. Click one of the Dashboard name links in the search results field to open a filtered view of the corresponding dashboard, which shows only the widget or object within a widget that you searched for. In the image below, an Object search was run using the search phrase testvserver.

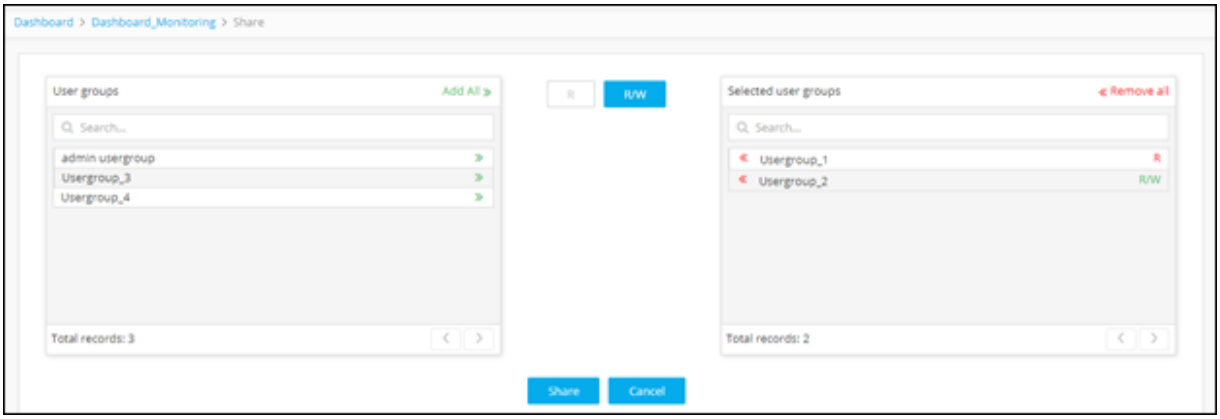


Share a Dashboard

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

To share a dashboard,

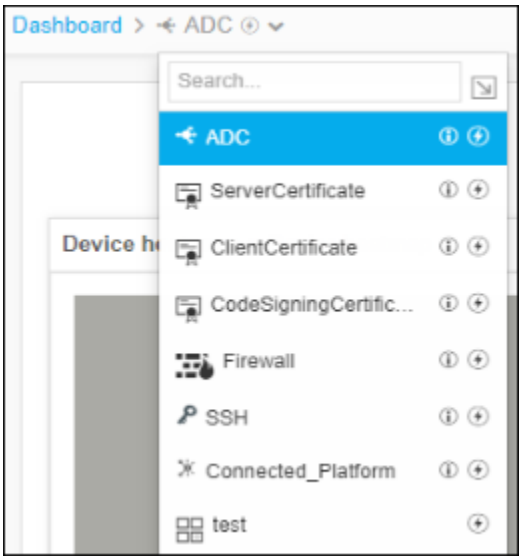
1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If you have more than one dashboard, in the dashboard table, click the name of the one you want to share.
3. When the dashboard opens, click the (**Share**) button in the Command bar at the top of the screen. The Share screen 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.

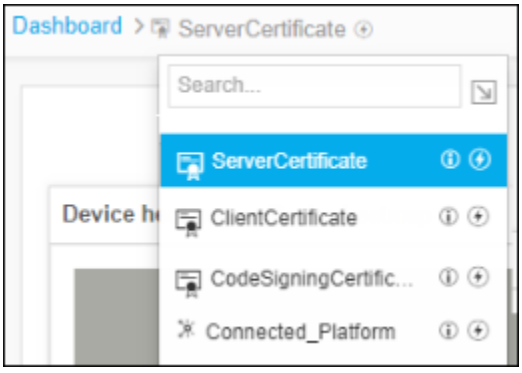


Switch Between Dashboards

To switch from one dashboard to another,

1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. Move your cursor to the breadcrumbs field of the current dashboard.
3. Click the current dashboard name.
4. In the dropdown list that appears, click the name of the dashboard you want to switch to.



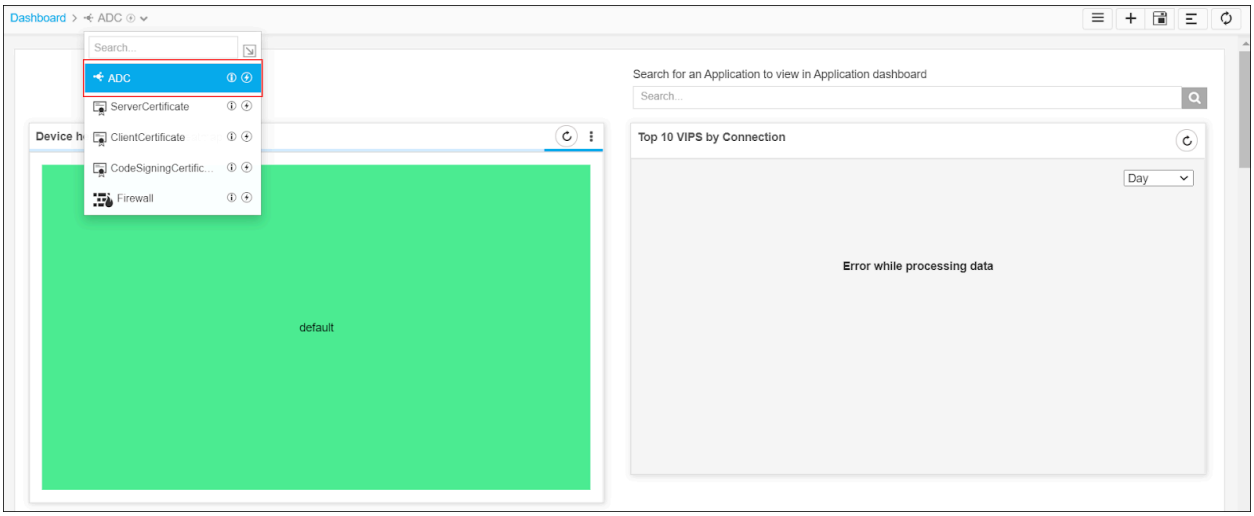


Note: You can also click the (**Dashboard inventory**) button in the Command Bar and click the name of the dashboard you want to switch to.

Default Dashboard

Users can get access to a pre-built Insights dashboard to monitor key application services KPI's/metrics.

Displays the pre-defined widgets to provide the usage reports and up-to-the-minute reports containing statuses and statistics for devices and certificates managed within the AppViewX platform.



The purpose of the key widgets is to:

- Monitor Device and Application health
- Monitor Top Applications Serving Maximum Traffic
- Monitor Unused Objects to Optimize LB Config
- Monitor App-centric Reports

AppViewX ships default dashboard called ADC available in dashboard inventory for monitoring the load balancing application managed in AppViewX.

This default dashboard is the landing dashboard screen by default. You can change the landing dashboard screen by clicking the icon beside its name.

Monitor Device and Application health on a Pre-Built Dashboard. Get better insights into the Device and Application health based on the statistical data configured for a specific interval.

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. The following reports are segregated and displayed as widgets on the ADC screen:

- Monitor Device and Application health
- Monitor Top Applications Serving Maximum Traffic

- Monitor Unused Objects to Optimize LB Config
- Monitor App-centric Reports

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

Monitor App-centric

Applications that contain traffic, bandwidth, status, success, and object count statistics are shown in the App-centric report. You can get to the App-centric report through either of the following paths:

- By entering the application name in the search bar of the ADC dashboard page. The App- centric report appears when you click one of the search results.
- By clicking any individual component (bar, pie wedge, grid square) in one of the following reports: Application heatmap, Top 10 applications by connections, and Top 25 applications by connections.

The App-centric report contains the following statistical widgets:

- **DNS Success Rate** - Displays statistics on the DNS success rate of applications based on the load balancing method.
- **Server Status Report** - Displays the status of all LTM pools.
- **Application Object Count** - Provides a pie chart showing the status of each object in the application.
- **Application Bandwidth Report** - Displays the overall bandwidth consumed by the application on an odometer.
- **Traffic Statistics Summary** - Displays the Virtual Server (VIP) level traffic statistics of a particular application for the period you choose. It provides the total traffic/connection served by the application.
- **VIP Level Traffic Statistics** - Displays the individual Virtual Server (VIP) level traffic details for the period (day/week/month/quarter) you choose. It is used to determine the highest traffic served per Virtual Server (VIP) and all the traffic/connections served by the Virtual Server (VIP) in that application.

Monitor Device and Application Health

The following heat map reports are used to monitor device and application Health:

- Device Heat Map
- Application Heatmap

Device Heat Map

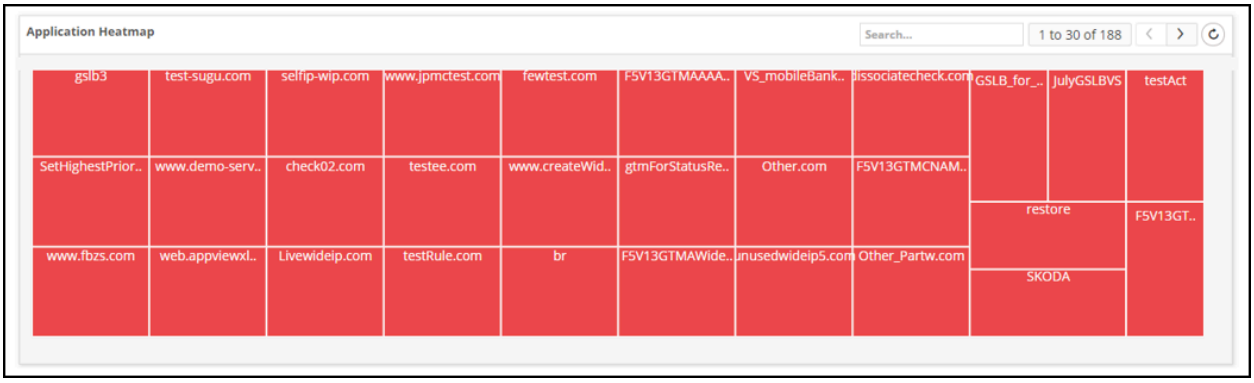
The device heat map is a graphical representation of the health of individual devices. The heatmap widget within the ADC dashboard displays each device group as a separate color block. When you hover your cursor over any device group block, a screen will pop up showing the number of Critical, Warning, Safe, and Not reachable devices available within the device group.

- If a device does not belong to any of the device groups in AppViewX, it appears in the default group block.
- When you click a device group block, the screen refreshes and displays all of the ADC devices available within the group as individual blocks.
- When you click on any device block, a screen appears displaying the memory, CPU, and bandwidth utilization, device info, logs, reports, and alarms for the respective device.

Application Heatmap

The application heatmap is a graphical representation of the status of an individual application, with each application displayed as a separate color block.

- When you click on any of the blocks, the respective App-centric report is displayed.
- When you hover your cursor over any of the blocks, the Application/Device name, State, Status, Success rate, and Object count are displayed.



Monitor Top Applications Serving Maximum Traffic

The top applications and their connections are monitored by the following reports:

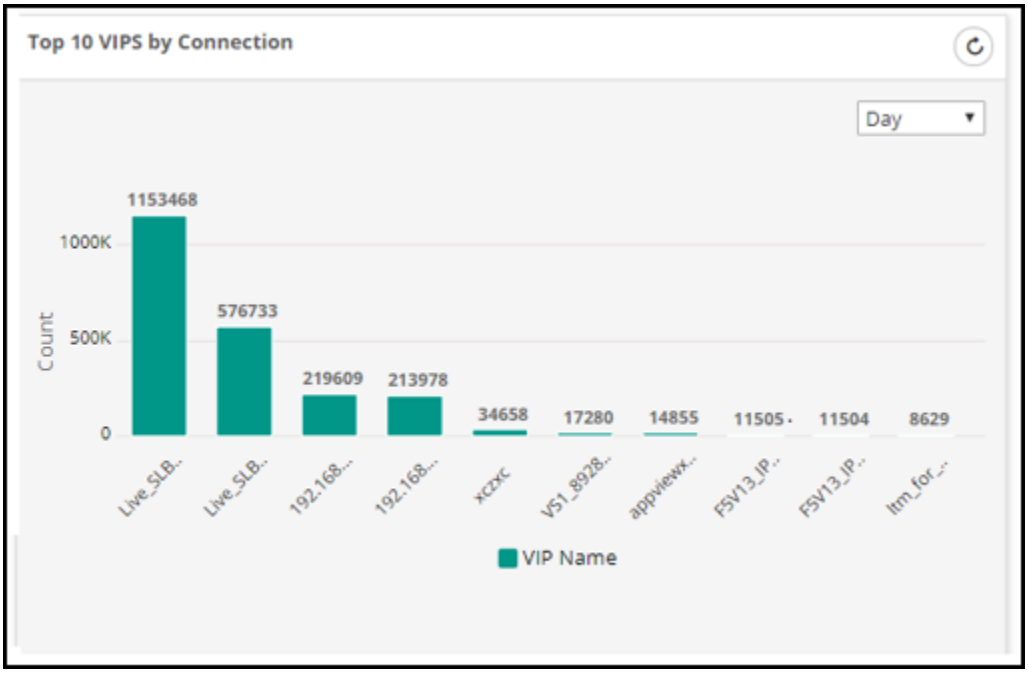
- Top 10 VIPS by Connection
- Top 25 Applications by Connection

Top 10 VIPS by Connection

A bar chart that shows the top 10 VIPs that currently has a maximum number of connections for a period (day/week/month/3 months) you choose.

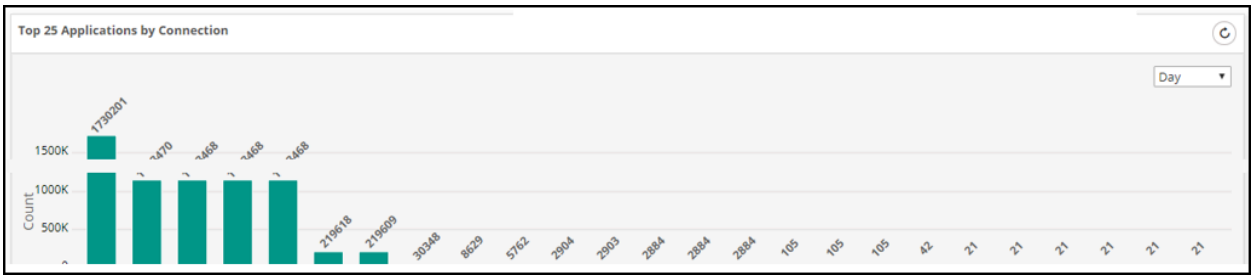
- When you click on any of the bars, the app search view of the ADC object is displayed.
- Application Heatmap - A graphical representation of the status of an individual application, with each application displayed as a separate color block.

- When you click on any of the blocks, the respective App-centric report is displayed.
- When you hover your cursor over any of the blocks, the Application/Device name, State,Status, Success rate, and Object count are displayed.



Top 25 Applications by Connection

A bar chart that shows the top 25 applications that currently have maximum connections for a period (day/ week/month/3 months) you choose. Each bar in the chart represents an application. When you click on any of the bars, the respective Appcentric report is displayed.



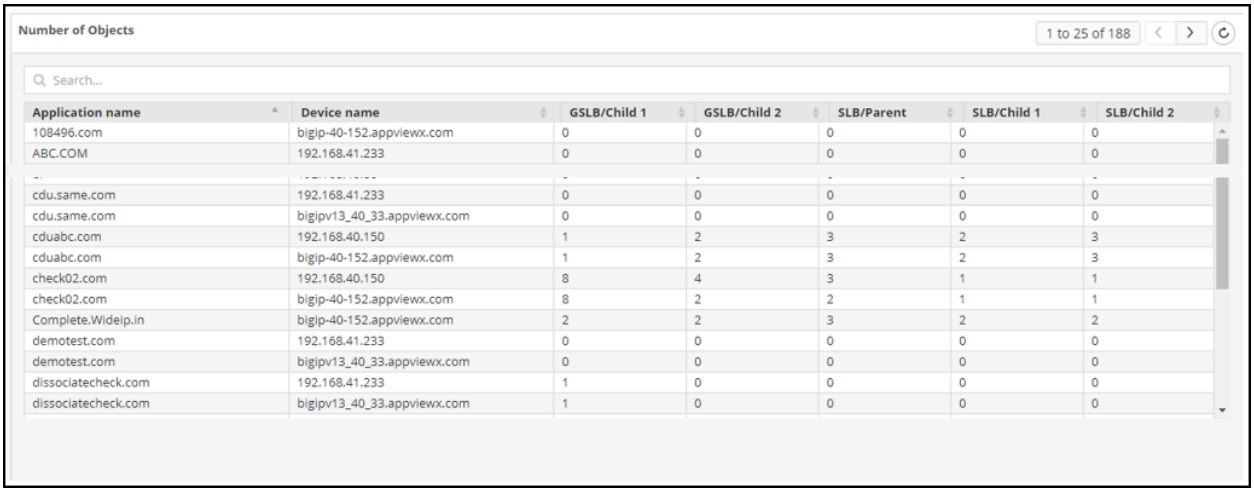
Monitor Unused Objects to Optimize LB Config

The following reports are used to monitor the unused objects in order to optimize LB configuration:

- Number of Objects
- Unused Objects Report

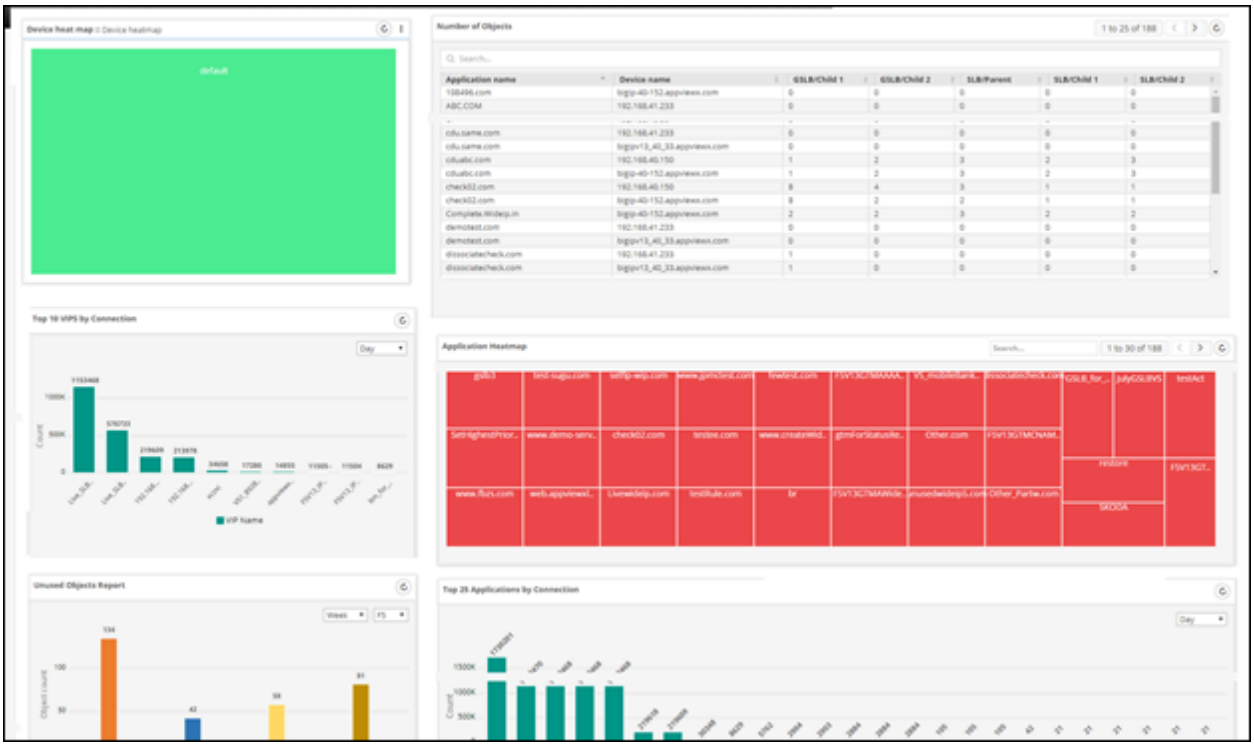
Number of Objects

It displays the total number of objects available in each application. It provides the number of children available for each object based on their hierarchy. When you click on any application name, the topological view of the object is displayed.



Unused Objects Report

A bar chart that shows the unused objects across all the active F5, Citrix, and A10 devices for a period (Week/Month/Quarter) you choose. This report helps users to scavenge unnecessary configurations of the device and manage configurations on the devices.



Custom Dashboard

The Netops users can design custom dashboard/app widgets in order to provide an overview of all the ADC devices and their objects within the AppViewX platform. A user can manage both the custom widgets and the default widgets that belong to multiple solutions (such as ADC, Certificate, Firewall, WAF, SSH, Visual Workflow, and AppVision) in the Dashboard that are created.

Manage and Monitor Application Traffic on Custom Dashboards and Widgets

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. It is highly flexible and enables you to create your own dashboards and share with selected users.

- Application View Widget
- Traffic Statistics Widget - Application Traffic Monitoring
- Traffic Grid Widget
- Script Execution (SE) Widget
- Class Management Widget
- Heatmap Widget

- Copy a Widget to Another Dashboard
- Move a Widget to Another Dashboard
- Delete a Widget
- Custom Widget

Application View Widget

- AppView Widget Overview
- Configure Application View Widget Using Predefined Layout
- Configure an Application View Widget Using a Custom Method
- Monitor and Manage Application Traffic
- Monitor Near Real-Time State/Status
- Search for an Object in an Application View Widget
- Modify an Application View Widget
- Enable or Disable Objects (appl.services) Displayed in a Widget
- Perform Bulk Actions on Objects in a Widget
- Force LTM Servers Offline Within a Widget
- View the Different Statuses and States for a Widget

AppView Widget Overview

Application view widget allows users to Route and Swing Traffic between Environments by logical grouping (datacenter based, device-based, WideIP VIP based, etc.) the service objects of the application. The widget displays the health of these objects, a number of connections, and other attributes. Provision to group the application based on business needs and Route/Swing Traffic between the environments accordingly.

You can perform the following actions on the widget::

- Configure an application view widget
- Monitor and manage application traffic
- Monitor near real-time state/status
- Search for an object in an Application view widget

- One-touch action provisioning and self-servicing
- Modify an Application view widget

Configure Application View Widget Using Predefined Layout

AppViewX offers Standard predefined templates for GSLB and SLB Applications management that allows you to create Instant Application Dashboards. By using the templates, the grouping of objects will be handled dynamically upon scaling of applications. This reduces the widget configuring time. Along with this the maintenance of the widget is also automated as the widget will be grouped automatically based on the layout selected. Follow three simple steps to create an App Dashboard quickly for your Application teams that enables seamless self servicing.

1. Choose the widget Layout/Application grouping format.
2. Configure Application patterns
3. Tag Widgets to a Dashboard

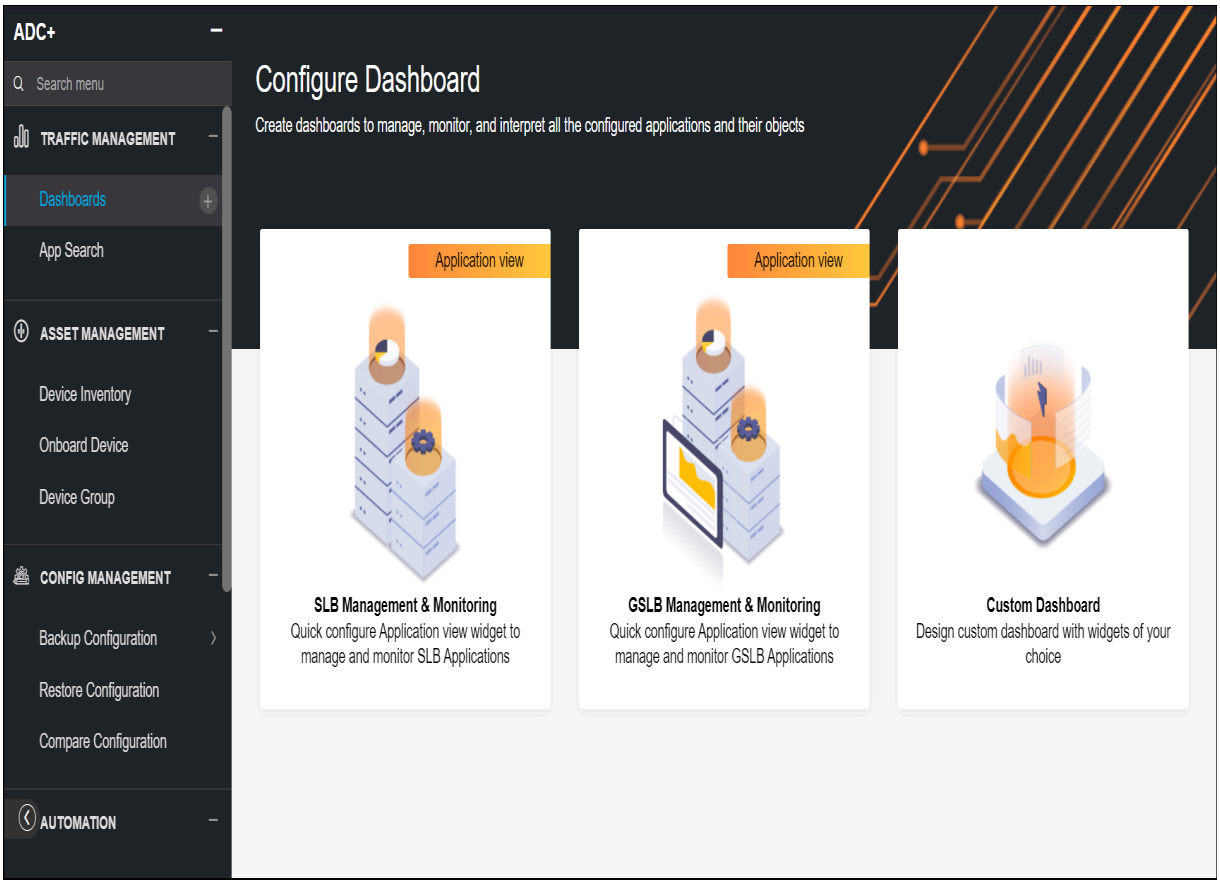
Gain instant visibility into your Applications across Devices, Data centers, Sync groups etc., in less than 30 seconds. With frequent change in addition and removal of applications, AppViewX ensures that the Dashboards are dynamic in nature and updates any change in the Application configuration instantly.

With AppViewX's granular and renewed RBAC, this becomes even more efficient as you can simply tag the rbac resources to the Dashboards. Application dashboards get dynamically created and updated exclusively for the users sharing the tagged resources.

Note: Even custom flavours can be created from this page using custom layout.

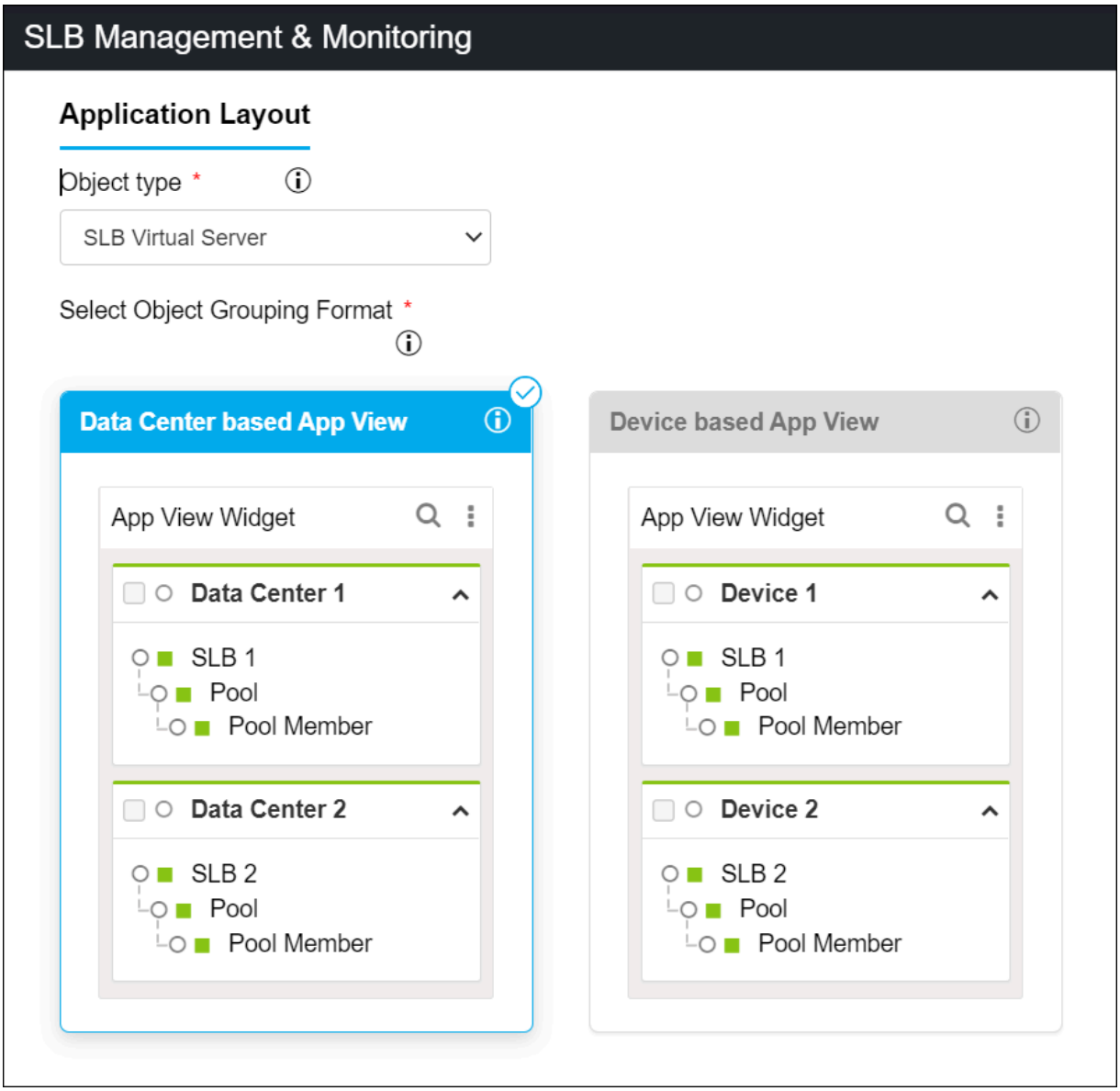
To configure an Application view widget using predefined layout,

1. Navigate to **menu** > **ADC+**.
   The ADC+ left navigation pane appears.
2. In the left navigation pane, click the add icon located beside **Dashboards**.
   The **Configure Dashboard** page appears. In this page, the layouts are categorized as follows:
   - SLB Management & Monitoring
   - GSLB Management & Monitoring



3. Hover the mouse over the desired layout category.
4. Click the **Use** button.

   The configuration page opens.
5. Select the field information in the **Application Layout** section:



6. The following table provides the field description for the **Application Layout** section:

Field	Description
Object Type*	Object type of the application. Select the kind of object you want to add. The options that appear in this field vary based on the selected option in the previous screen.
Select Object Grouping Format*	Choose how the applications should be grouped within the widget. The above image depicts how

Field	Description
	the applications will be grouped within the widget. The options are as follows: • **Data Center View** - select this option to group the applications based on the value given while adding the device. • **Device View** - select this option to group the applications based on device name.

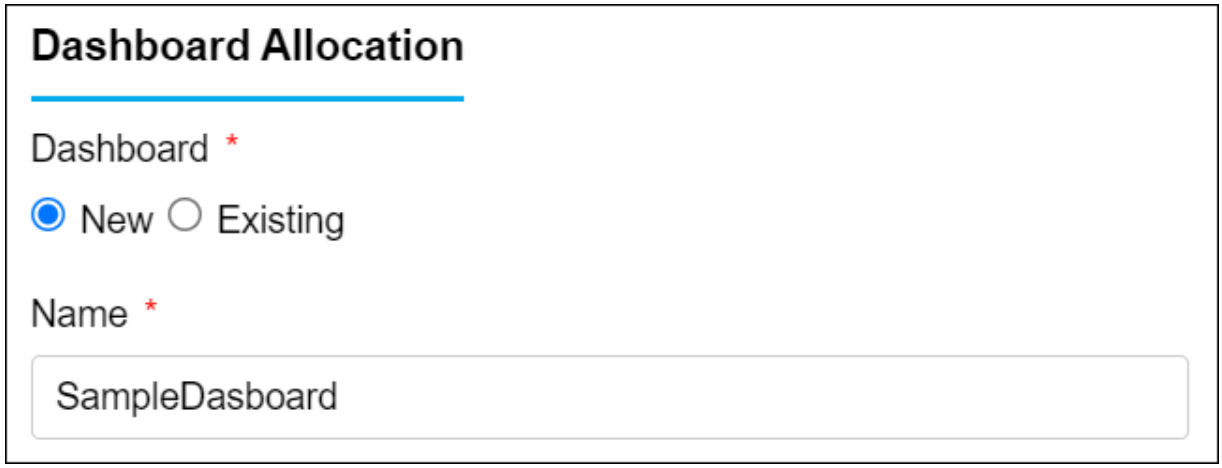
7. Enter or select the field information in the **Add Objects** section.

8. The following table provides the field description for the **Add Objects** section as follows:

Field	Description
Name	Name of the widget.
Add Resource (or) Add Objects	**Add Resource** - Click this button to configure the widget with a resource, which is already configured within AppViewX in **Accounts** > **Resource** page. By doing this, any updates made to the resources will automatically be seen in the widget as well. **Add Objects** - Click this button to add objects manually or use specific regex patterns so that any new applications matching the given regex will automatically be added to the widget.

Field	Description
	Note: Only 1000 objects can be included in each widget.
Add Widget	Click this button to configure one more widget with the same layout selected. Maximum of three widgets can be created for a layout.

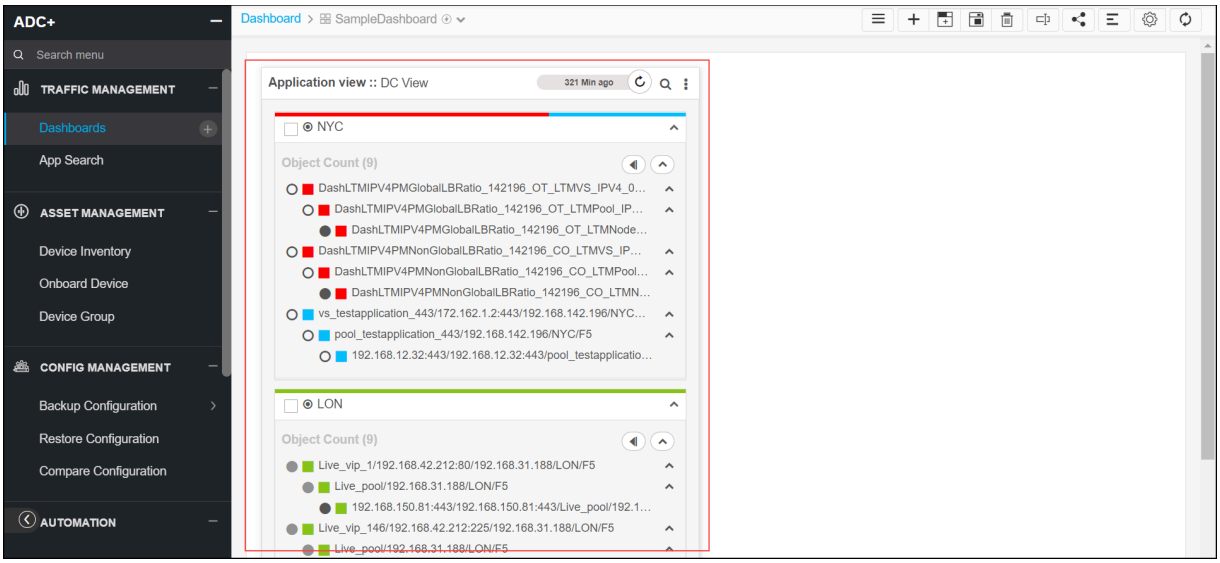
9. Select the field information in the **Dashboard Allocation** section.



10. The following table provides the field description for the **Dashboard Allocation** section as follows:

Dashboard*	Select the **New**/**Existing** option to either create a new dashboard or select an existing dashboard into which newly created widget(s) to be added. **Note:** When you select **New** dashboard option, you need to provide name for the Dashboard.

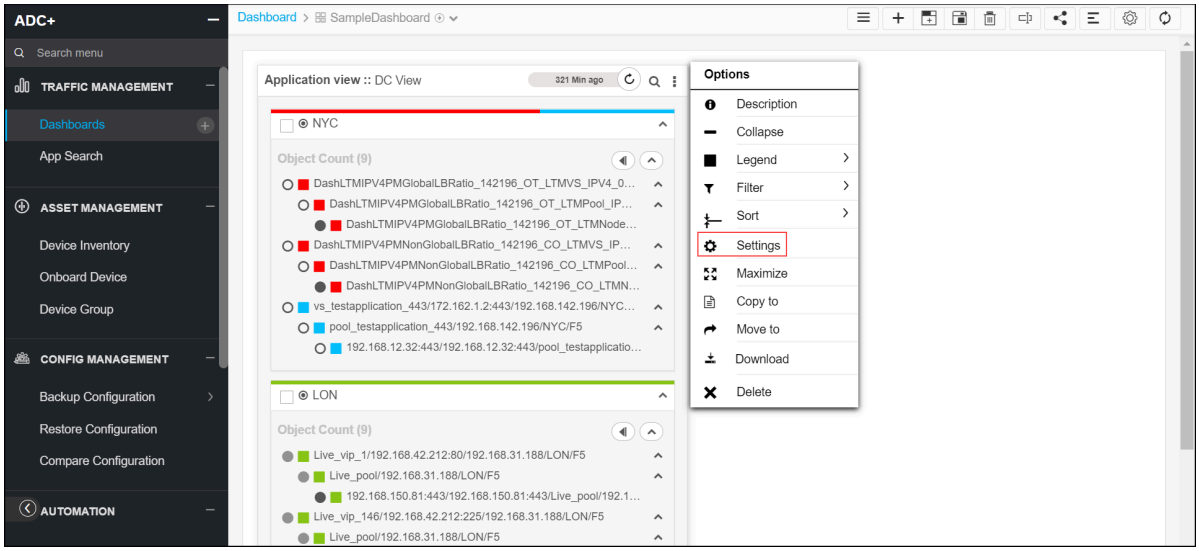
11. Click the **Create** button.
    The widgets are created and you will be landed in the dashboard. You can see the widgets created with the input applications grouped based on the layout selected.



12. To reconfigure the applications or to change the layout,

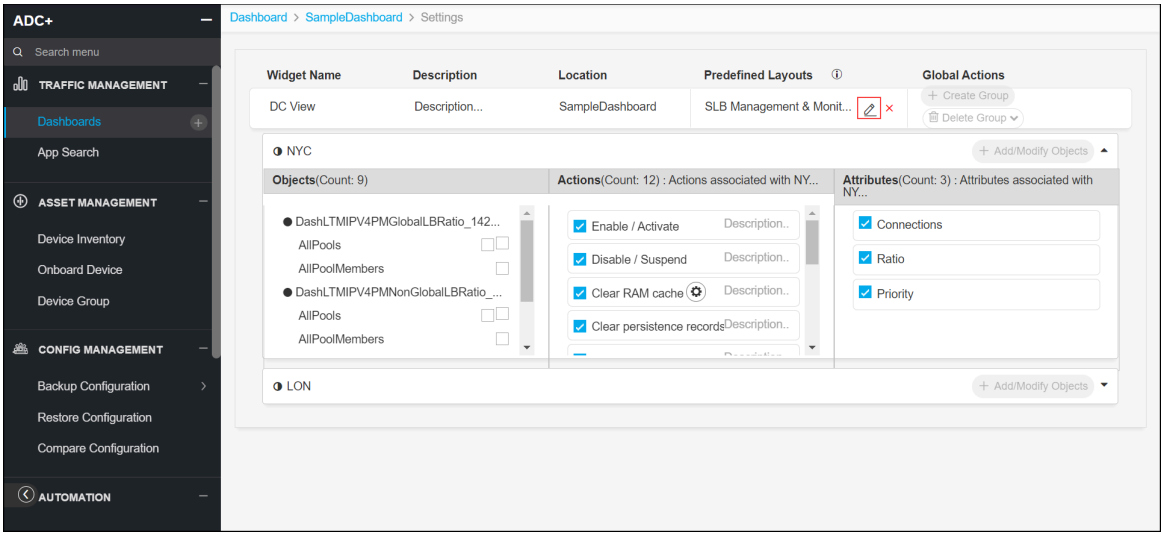
> **Note:** For a widget configured with layout, you cannot add/delete objects or perform any group level actions from the below screen as the groups are updated dynamically based on layout selected.

- Select the **Setting** icon from the dashboard options.



- To change the layout,

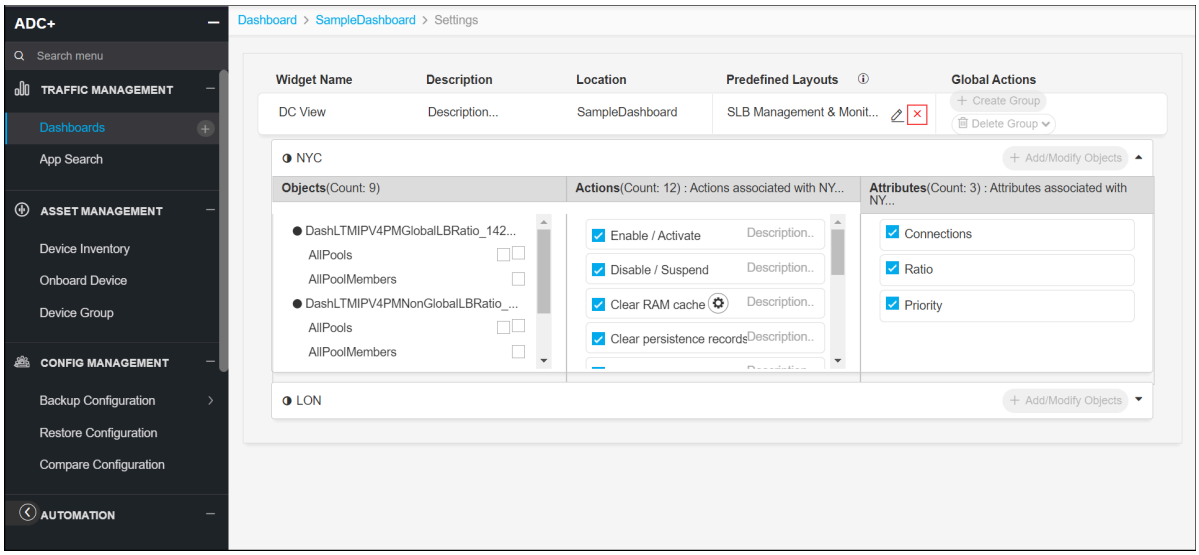
a. Click the edit icon.



The configuration page opens.

b. Change the layout in the configuration page, and then click the **Update** button.

- To remove the applied layout, click the delete icon, and the click the **Proceed** button in the confirmation pop-up.



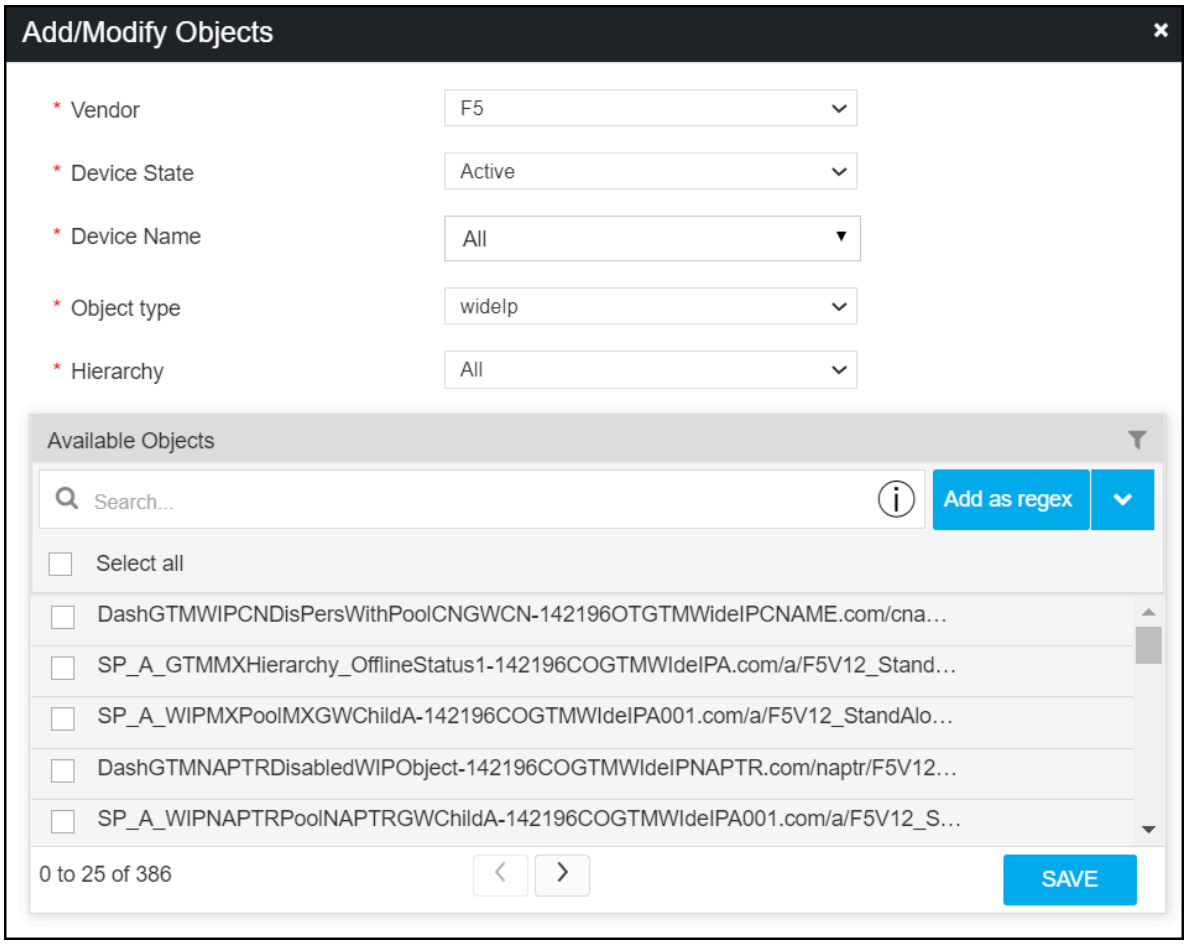
Note: Removing the layout converts the widget to a custom layout and the associated widget group will no longer update dynamically.

Configure an Application View Widget Using a Custom Method

To configure an Application view widget using standard method,

1. If you are creating an Application view widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic, then jump to Step 5 below. If you are creating an Application view widget for an existing dashboard, click the  (**Add widget**) button in the Command bar of the dashboard.
2. On the **Create** widget screen that pops up, select the solution ADC from the dropdown list.
3. Select the **Custom** radio button as the type of widget.
4. Select the Application view as the widget you will be creating.
5. Enter a unique name for the widget.
6. Click **Create**.
7. The **Settings** screen for the Application view widget opens, displaying an empty DefaultGroup where the user can add the objects.
   For example, In order to Monitor SLB objects of specific applications, start creating groups in the name of the Application and add SLB objects into required groups.
8. Modify the widget name, group name, and add a description by clicking the corresponding fields. It will then become a text-entry field that allows you to make changes.
9. Add objects to the group for the widget one of the following ways:
   - manually
   - using regex
10. Add objects manually to the group for the widget as follows:

a. Click the **Add/Modify Objects** button to add the objects at the group level. Select the vendor from the **Vendor** dropdown list.



b. In the **Device State** field, select whether you want to include devices in the widget that have a status of Active, Standby, or All, where "All" means devices with a status of either Active or Standby.

c. In the **Device Name** field, select the device name whose objects you want to add to in the widget.

d. In the **Object type** field, select the kind of object you are adding. The options that appear in this field vary depending on the vendor you selected.

e. In the **Hierarchy** field, select the required level of hierarchy that should be displayed in the dashboard. The options that appear in this field vary depending on the vendor and the object type you selected. The objects based on your selection will be displayed in the Available Objects table at the bottom of the screen.
For example, A WideIP object will have the following hierarchical types,

- **All** - WideIP along with all hierarchical objects like Pools and Pool members.
- **All Pools** - WideIP along with the Pools.
- **All Pool Members** - WideIP along with the Pool Members.
- **WideipOnly** - WideIP only without any hierarchy.
- **None** - No objects will be explicitly listed on the widget. Instead, only the state/status of the objects will be represented on the widget for monitoring.

f. Select the checkbox beside the object name and click **SAVE** to add the objects to the group.

11. Add objects via regex to the group for the widget as follows:
    a. Click the **Add/Modify Objects** button to add the objects at the group level. Select the object filter details such as **Vendor**, **Device State**, **Device Name**, **Object type**, **Hierarchy**.

    The objects that match the filter details are displayed.

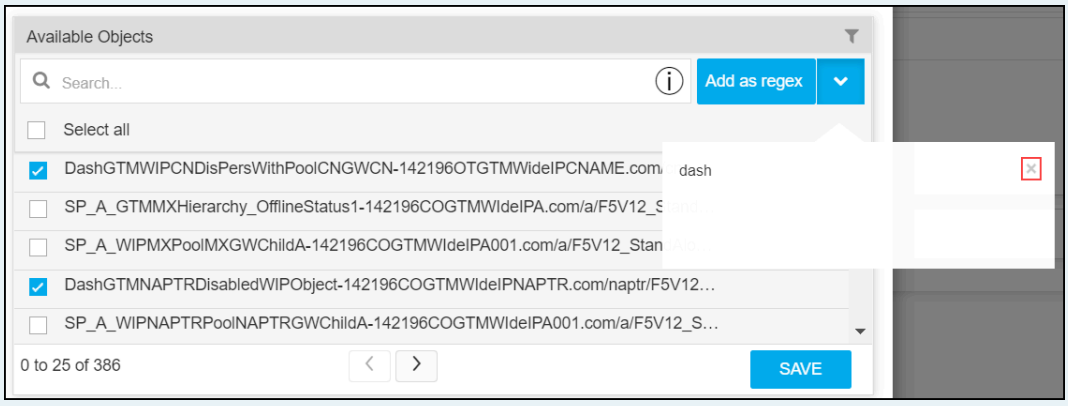
    b. Add regex in the **Search** field, and then press **Enter**.

    The objects that match regex are displayed.

    c. Click the **Add as regex** button.
    The displayed objects are added to the group, the regex is added to the list, and it can be used whenever it is needed.

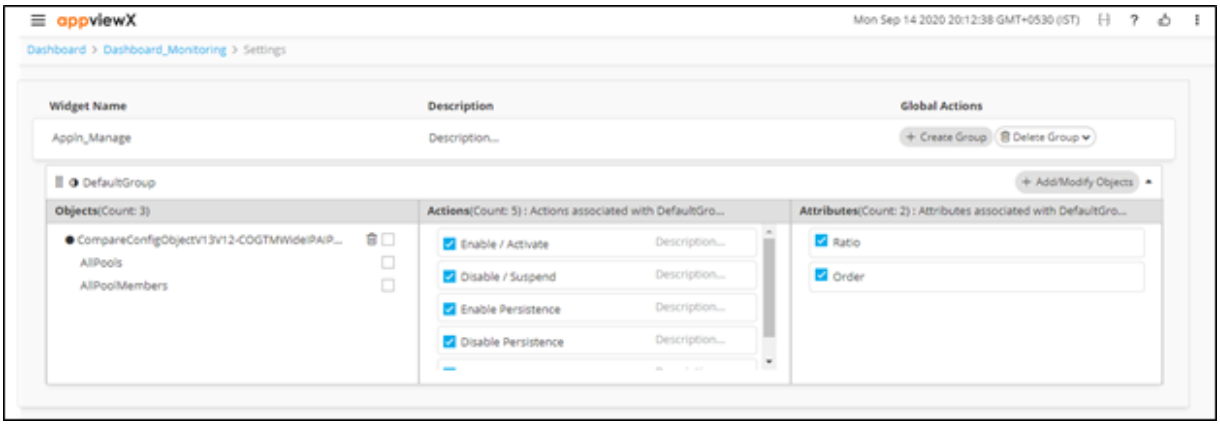
Note:

- You can add any number of regex. To view the list of regex, click the **Add as regex** dropdown option.
- The regex(s) is specific to a widget, dashboard, group, and filters.
- To delete a regex from the list, click the close button against the regex in the list.

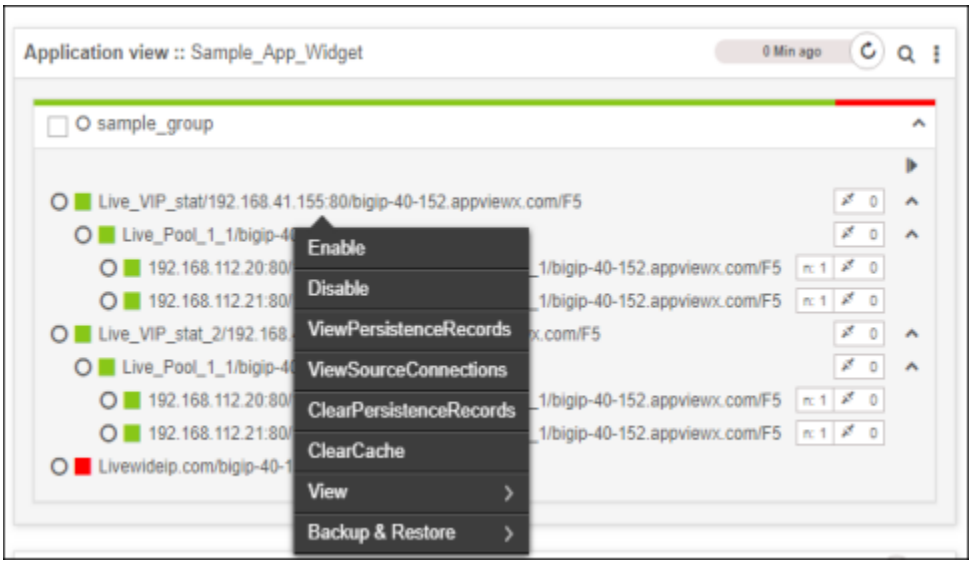


- To view sample regex, click the information button.
- When new objects are added and matched with the regex the objects are added to the widget automatically.

12. The Actions and Attributes corresponding to objects added will be automatically listed in their respective sections.
13. For example, you might grant group members actions (such as Enable, Disable, ForceDown, and so on) and attributes (such as Ratio, Order, Weight, Connections, and Priority) permissions to one object in a group, but only Enable, Disable, and Ratio permissions to another object in the group and no permissions to objects in a sub-group of the group.
14. When the widget appears on the dashboard, the full list of actions you created can be accessed by right-clicking any object within the widget.
15. Click on the or (**Show/Hide Attributes**) button to view or hide the full list of attributes you created for a group.
16. When you have finished, click **Save**.
    The Application traffic can be managed and monitored.



17. The dashboard screen reappears, displaying the widget you just created.



18. To create a new group,
    a. Click the **Create Group** button under Global Actions.
    b. On the pop-up that appears, enter a group name to help the users identify it.
    c. Select the parent that you want to associate with the group from the dropdown list.
    d. Click **Save**.
    e. Repeat steps 7-15 to include the group in the dashboard.
19. To delete a group, complete the following steps:
    a. Click the **Delete Group** dropdown menu under Global Actions.
    b. Select the groups that you want to remove from the widget and click **Delete**.

Monitor and Manage Application Traffic

The widget with the configured Application along with its hierarchy will be rendered onto your dashboard and start monitoring the Applications State/Status. The following Legend helps to identify the state/status definition, click the ⋮ (**Options**) button and select legend in the Command bar at the top of the widget.

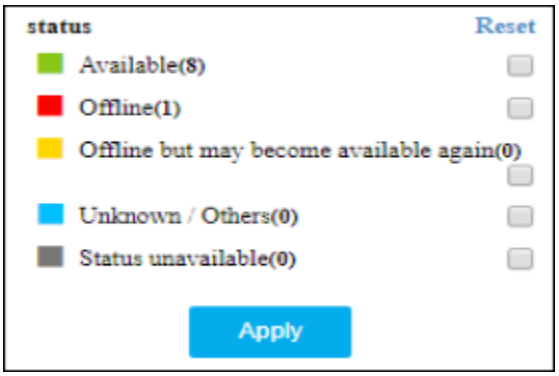
The applications can be,

- Filter the Applications
- Sort the Applications

Filter the Applications

To filter the applications based on the status,

1. Click the ⋮ (**Options**) button and select the ▼ (**Filter**) icon in the Command bar at the top of the widget.
2. In the Status field that appears, select the checkboxes beside the Status info that you would like to filter.



The applications that match the filtered status appear on the screen.

Sort the Applications

To sort the applications in ascending/descending order,

1. Click the (**Options**) button and select the (**Sort**) icon > Ascending/ Descending in the Command bar at the top of the widget.
   The objects are arranged and displayed in the corresponding order.
2. Click the **Save Dashboard** icon to retain the sorting.

Monitor Near Real-Time State/Status

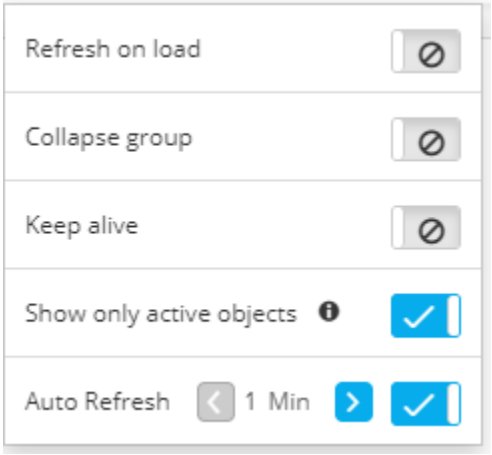
Monitor the near real-time state/status of your applications from the Application view widgets ensuring a seamless experience.

Note:
AppViewX recommends to enable Syslog-based configuration updates for near real-time monitoring. Refer to Installation Guide for enabling Syslog configuration.

You can enable the below options in the Dashboard settings for near real-time monitoring. For Dashboard setting, see Dashboard Setting section.

- **Refresh on load** - Enables Refresh on load from the (**Settings**) of the dashboard page to get the latest state/status information on loading the dashboard.
- **Last Refresh time** - Displays the last time the widget is updated with the latest State/Status information.
- **Refresh** - Click the **Refresh** button on the widget to perform on-demand State/Status information. Each Object contains a last refresh time on the tooltip, you can also trigger a refresh for a particular object from the tooltip.
- **Collapse group** - If this setting is enabled, each time the dashboard loads, all groups within widgets on the dashboard display in a collapsed state by default.
- **Collapse hierarchy** - If this setting is enabled, each time the dashboard loads, all object hierarchy within widgets on the dashboard display in a collapsed state by default.

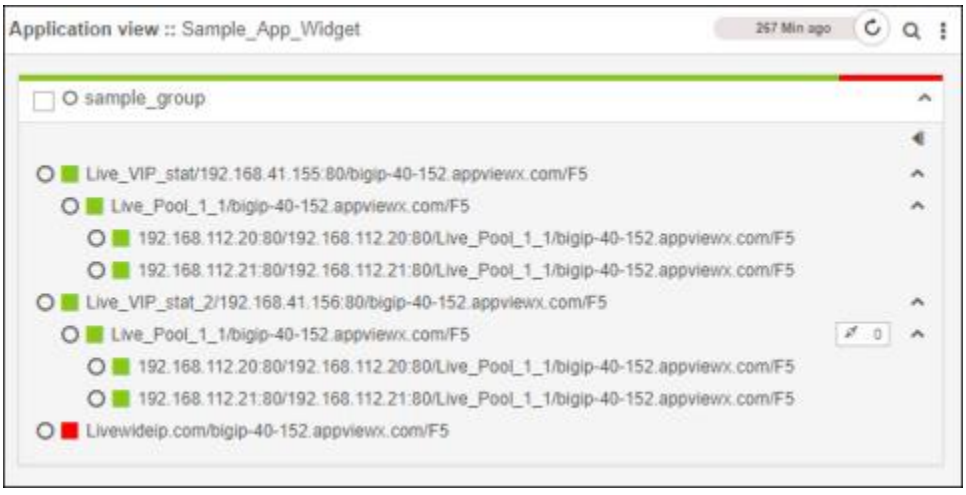
- **Keep Alive** - This option is available in the dashboard **settings** . If this option is enabled, it ensures the session is not timeout by refreshing the dashboard every 15 mins.



- **Show only active objects** - If this option is enabled, only the active objects are displayed within the widget.

Example, in the following sample application widget,

- all of the objects in the widget show that they are in an Enabled state-they all have hollow circles beside their names
- one of the InternalDMZ-Members objects is offline, so it shows a red square beside its name, indicating its Offline status.
- Three of the other objects display gray squares, indicating their Unlicensed/None/Failure States status.



- The temperature bar, which is the colored bar at the top of each group or object name, displays the overall status of all components within the widget. In the example above, note that the virtual server group shows a solid green temperature bar because all components under it are Available, whereas the Members group shows a mostly green bar transitioning to red, to indicate that some of the components within it are Unavailable. Hover your cursor over the color in the temperature bar to see the number of components that have the corresponding status.

Search for an Object in an Application View Widget

To search for an object in an Application view widget,

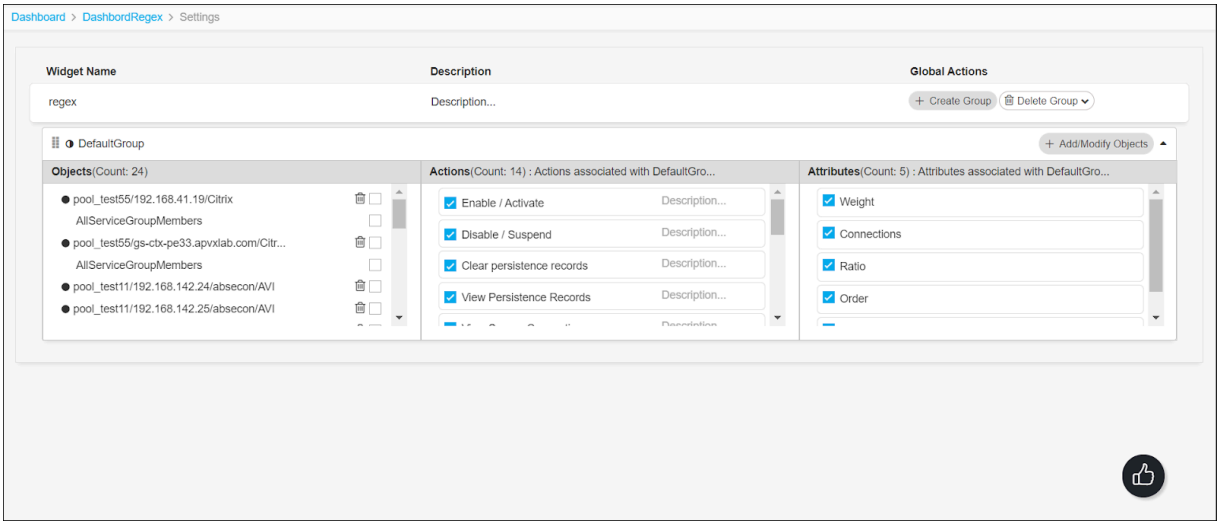
1. Go to ☰ **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If you have more than one dashboard, in the dashboard list, click the name of the one containing the widget you want to search.
3. In the widget Command bar, click the 🔍 (**Search object**) icon.
4. In the search field that pops up, begin entering the name or number of the object you want to find.
5. As you enter text in the search field, the contents of the widget update dynamically to display only those objects that match the characters or numbers entered so far. In the example below, the only objects remaining in the widget are those that contain the letters entered into the search field: best. All other objects have been filtered out.

Modify an Application View Widget

The Application view widget contains the objects under the group. By default, the DefaultGroup is available. Either you can add objects to the DefaultGroup or create a new group of objects. The details of the Application view widget can be modified as needed.

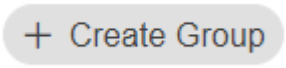
To modify an Application view widget,

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 containing the widget whose contents you want to make changes to.
3. Click the (**Options**) button and select the (**Settings**) icon in the Command bar at the top of the widget.
   The Settings screen appears:



4. You can modify the Application view widget as follows:

Field	Description
Widget Name	Update the name of the widget.
Description	Update the description of the widget.
Global Actions	There are two Global Actions. Click,

Field	Description
	•  to create a new Application view widget group. •  to select the desired group from the drop-down list and delete.

Add/Modify Objects	• Click  to add and modify an object.
	• In the **Add/Modify Objects** popup, provide the object details, such as vendor, Device State, Device Nam, etc., search for objects, and/or filter the objects to get the desired objects.
	• Select or unselect the objects by clicking the objects checkbox.
	• Alternatively, you can add objects to the group by creating regex for the object details to get the desired objects. To add objects using regex,
	  • After providing the object details in the **Add/Modify Objects** popup, add the desired regex in the search field.
	  • Click the **Add as regex** button.
	  The objects that match the regex are added to the group and the regex is added to the regex list.
	  Note:
	  • You can add any number of regex.
	  • To view the regex list, click **Add as regex** dropdown option.
	  • The regex(s) is specific to a widget, dashboard, group, and filters.
	  • To view sample regex, click the information  button.
	  • When new objects are added and matched with the regex the objects are added to the widget automatically.
	• Click **Save** to add the objects to the group.

Objects section	To delete an object, click  against a particular object and then click **Yes** in the confirmation modal.

Field	Description
Actions section	Enable or disable action(s) for the objects by selecting the checkbox of the respective action. The enabled actions will be updated in the action list. By default, access to the actions applies to all objects within that group.
Attributes section	Enable or disable attribute(s) for the objects by selecting the checkbox of the respective attribute. By default, access to the attributes applies to all objects within that group.

5. The modified details will be updated in the Application view widget.

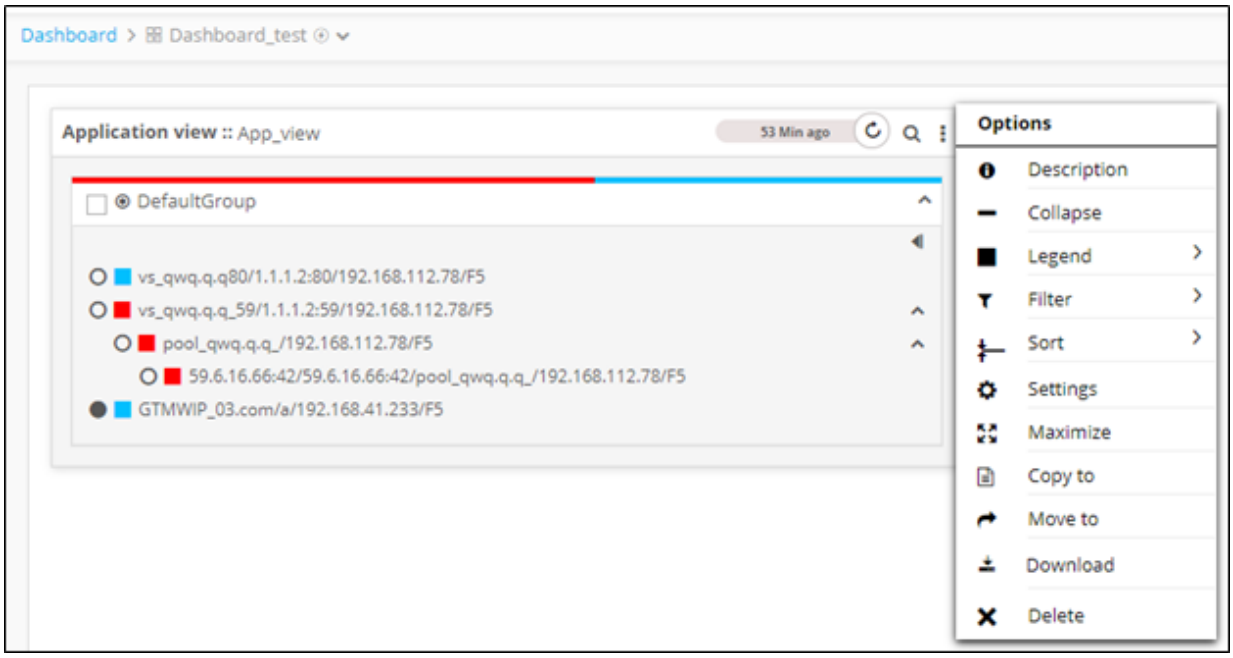
- One-Touch Action Provisioning and Self Servicing
- Actions on HA Devices and Device Failover

One-Touch Action Provisioning and Self Servicing

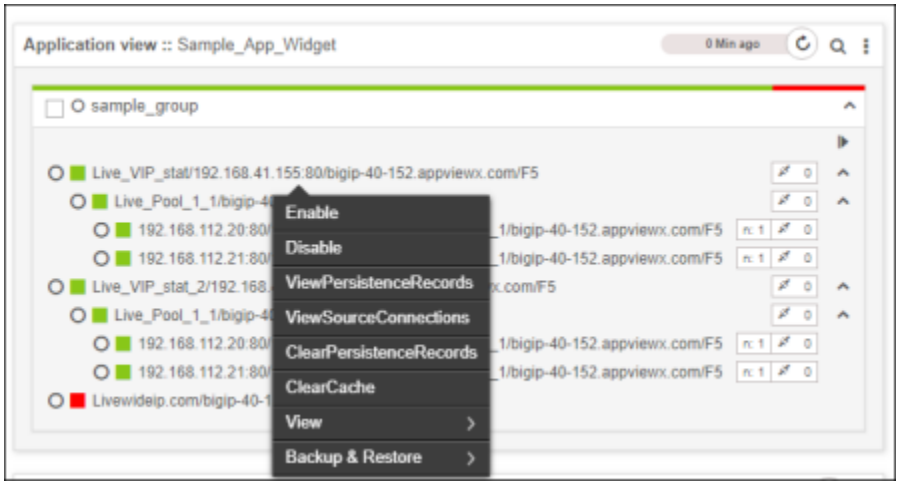
- The app-centric dashboard/widget allows you to self-service, monitor, and troubleshoot application issues in a single pane.
- One-touch/click application provisioning and Traffic management actions through a simplified RBAC.

The configured objects along with their hierarchy are rendered in the form of a widget.

- Users can Expand and Collapse the group by Clicking the ⋮ (**Options**) button.



- Execute Server Rotation or Route/Swing traffic between your environments and perform various other operations on a single click.



The following actions can be performed (**Individual or bulk**) on an Application View widget by right-clicking the Group/Individual object and accessing the Actions menu:

- **Enable** - Enable an object
- **Disable** - Disable an object and terminate all active connections

- **Graceful disable** (AVI devices only) - Disable an object only when all the currently active client connections are closed by either the server or the client
- **Backup & Restore**
  - **Backup device** - Create a backup of the device associated with the object. For more details refer to the Create a Device Backup Group section of this guide.
  - **Restore object** - Restore object configuration to a previous state. For more details refer to the Restore an Object section of this guide.
  - **Compare** - Compare current and/or archived configurations of similar objects or across devices to ensure compliance. For more details, refer to the Compare ADC Objects section of this guide.
- **View**
  - **View graph** - View the timeline statistics of an object. For more details, refer to the View Timeline Statistics for an Object section of this guide.
  - **View config** - View the current configuration of all levels of the device object. For more details, refer to the View Configuration Details section of this guide.
  - **View log/history** - View the log history of the object.
  - **View alerts** - View any alerts related to the object.
- **Clear persistence records** (F5 devices only) - Clear the persistence records for Virtual Server (VIP) and pools
- **View persistence records** (F5 devices only) - View the persistence records for Virtual Server (VIP) and pools
- **Advanced**
  - **Enable/Disable persistence** (F5 devices only) - Turn on or off 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.
  - **Enable/Disable all** (F5 devices only) - Turn on or off the object available across all the pools.
  - **Forcedown all** (F5 devices only) - Force shutdown of the object available across all the pools.
- **View source connections** (F5 devices only) - View the source connection IPs for Virtual Server (VIP) and pools
- **Forcedown** (F5 devices only) - Force shutdown of the object
- **FD clear active connections** (F5 devices only) - Clear active connections to the object
- **View Topology** - Display the topology view of the selected object in a new window

The following are the additional attributes that can be monitored on the widget,

- **Ratio** - To view the ratio of the pool member from widget level
- **Weight** - To view the real server weight for the applicable objects from widget level

Actions on HA Devices and Device Failover

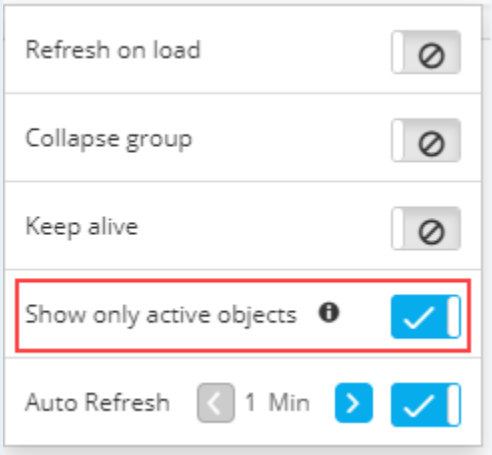
AppViewX recommends to enable Syslog-based configuration updates to reflect the device flip over on a near real-time basis.

To enable the Syslog based configuration updates,

- Enable **Show only active objects** option from the Dashboard settings.

  It ensures the widget is always updated with the latest active device objects whenever a device failover is identified.

Note: By default, this option is enabled.



- To disable this option, click the ⚙ (**Settings**) icon on the dashboard page.

Note: In addition to this, any actions that are executed on an application hosted on a HA device will always be reflected on the current active device to ensure the active devices are up to date and no changes are overwritten during device synchronization. AppViewX also ensures the Active and Standby devices are synchronized at a regular interval.

Following are other actions that can be performed by clicking the **Options** on the widget,

- Maximize
- Minimize
- Copy to - a copy of the widget can be placed from one dashboard to another dashboard by selecting the (**Copy to**) icon under (**Options**).
- Move to - any widget can be moved from one dashboard to another dashboard by selecting the (**Move to**) icon under (**Options**).
- Download - contents of an Application view widget can be downloaded in .csv format to your local system by selecting the (Download) icon under (**Options**).
- Delete - a group, object, or action can be deleted from an Application view widget by selecting (**Options**) > (**Settings**) > **Groups/Objects/Actions**, and then click **Delete**.

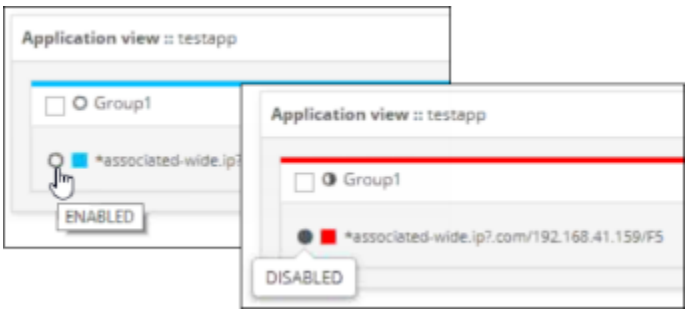
Note: Every Group must have at least one action associated with it, so if there is only one action listed, the Delete button will not be enabled.

Enable or Disable Objects (appl.services) Displayed in a Widget

Application teams can quickly perform provisioning, server rotation as part of a standard change window by enabling or disabling the objects.

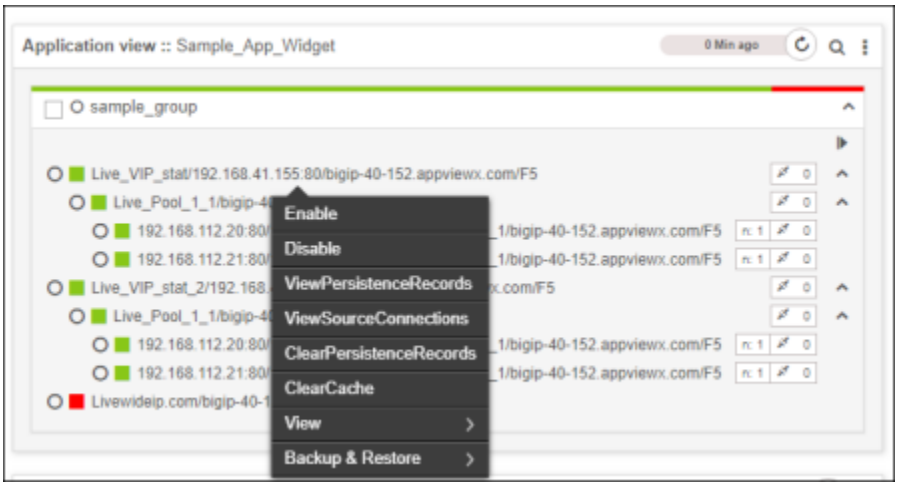
Note: This process can be integrated into ITSM change management.

Objects that are enabled within a widget contain an open circle beside their names and display the word ENABLED when you hover your cursor over the circle. Objects that are disabled contain a filled black circle beside their names and display the word DISABLED when you hover over them.



To enable or disable objects displayed in a widget,

1. Go to ☰ **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If the specific dashboard you want to access is not displayed on the screen, move your cursor to the breadcrumbs field of the current dashboard.
3. Click the current dashboard name.
4. In the dropdown list that appears, click the name of the dashboard you want to switch to.
5. When the dashboard opens, locate the widget that contains the object whose status you want to change.
6. Right-click the object and select **Enable** or **Disable** from the dropdown menu that appears.



7. On the Confirmation screen that pops up, enter comments relating to the enable or disable action, then click **Yes**.
8. Click the ↻ (**Refresh**) icon in the widget Command bar to see the updated view of the widget.

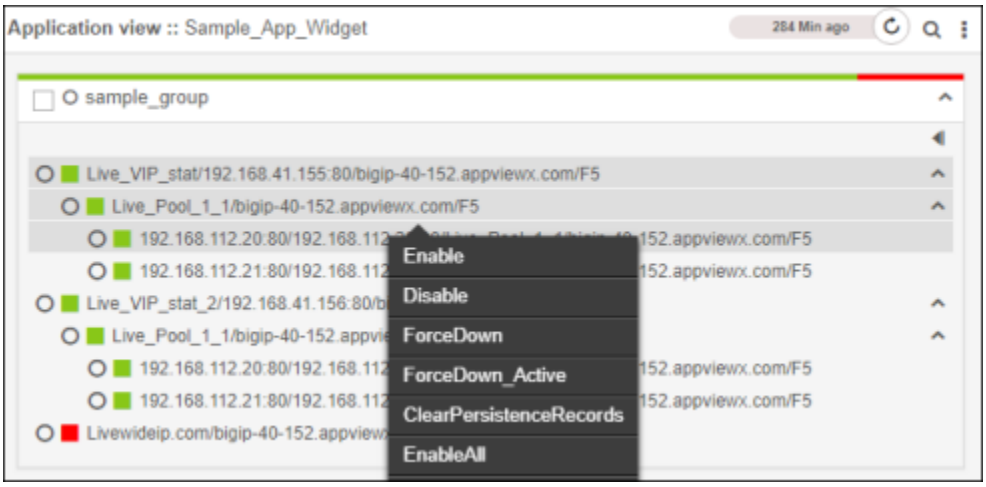
Perform Bulk Actions on Objects in a Widget

The Dashboard module allows you to perform the same action on multiple objects within the same widget simultaneously.

To perform bulk actions on objects in a widget,

1. Go to ☰ **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If the specific dashboard you want to access is not displayed on the screen, move your cursor to the breadcrumbs field of the current dashboard.

3. Click the current dashboard name.
4. In the dropdown list that appears, click the name of the dashboard you want to switch to.
5. When the dashboard opens, locate the widget containing the objects that you want to perform bulk actions on.
6. Click on each object within the widget that you want to perform a bulk action on. If you want all objects in the group to be included, select the check beside the group name.
7. Right-click anywhere in the widget and select the action you want to perform from the dropdown menu.



8. On the Confirmation screen that pops up, enter comments related to the action you are performing, then click **Yes**.
9. Click the ↻ (**Refresh**) icon in the widget Command bar to see the updated view of the widget.

Force LTM Servers Offline Within a Widget

During server maintenance, it is sometimes necessary to force a Local Traffic Management (LTM) server within a widget. When this is done, the server is still able to serve existing active connections, but no new connections are processed.

To force an LTM server offline within a widget, complete the following steps:

1. Go to ☰ **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. If the specific dashboard you want to access is not displayed on the screen, move your cursor to the breadcrumbs field of the current dashboard.
3. Click the current dashboard name.
4. In the dropdown list that appears, click the name of the dashboard you want to switch to.
5. When the dashboard opens, locate the widget that contains the LTM server you want to force offline.

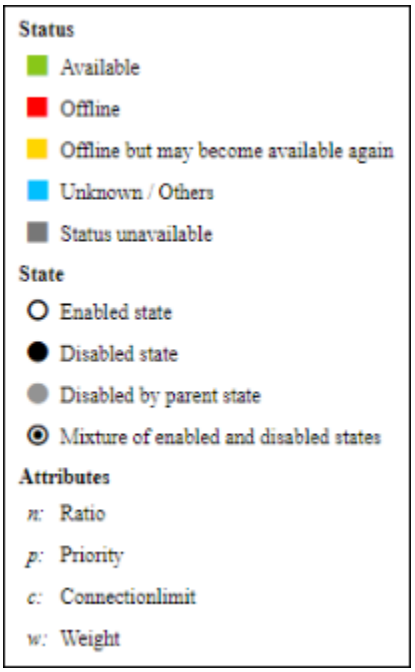
6. Click the LTM server name in the widget, then right-click and select Forcedown from the dropdown menu that appears.

7. On the Confirmation screen that pops up, enter comments relating to the force-down action, then click **Yes**.
8. Click the (**Refresh**) icon in the widget Command bar to see the updated view of the widget.

View the Different Statuses and States for a Widget

To see a list of all of the statuses an Application view or Traffic grid widget can have, complete the following steps:

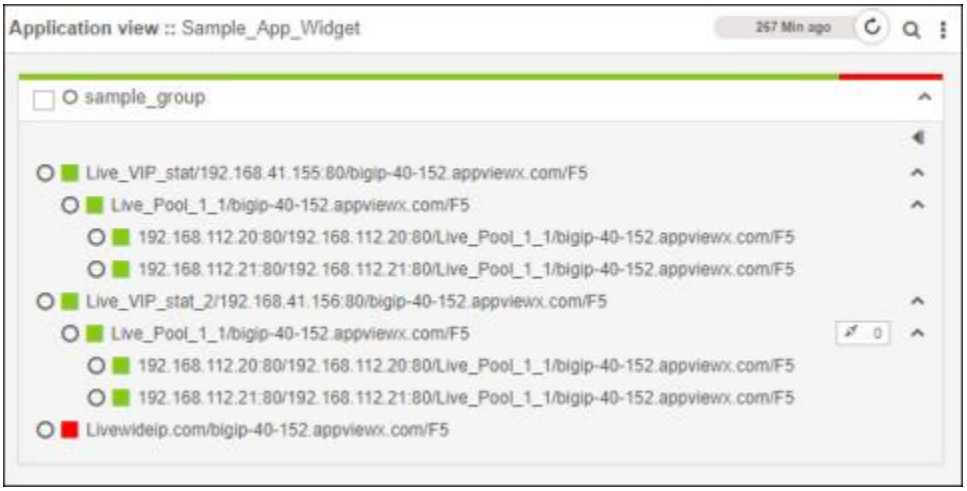
1. Go to **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **Dashboards**.
2. Select a dashboard that has an Application view or Traffic grid widget.
3. Click the (**Options**) button and select (Legend) icon in the Command bar at the top of the widget.
4. A legend appears, listing each of the possible widget statuses and states. For Application view widgets, there are five possible statuses and four possible states, as shown below.



5. The list for Traffic grid widgets is larger, with a total of 9 possible statuses and 6 possible states, as shown below.

6. Using this legend, you can tell at a glance the current status and state of each component of the widget. In the Application view widget example below, all of the objects in the widget show that they are in an Enabled state-they all have hollow circles beside their names-but one of the InternalDMZ-

Members objects is offline, so it shows a red square beside its name, indicating its Offline status. Three of the other objects display gray squares, indicating their Unlicensed/None/Failure States status.



7. The temperature bar, which is the colored bar at the top of each group or object name, displays the overall status of all components within the widget. In the example above, note that the virtual server group shows a solid green temperature bar because all components under it are Available, whereas the Members group shows a mostly green bar transitioning to red, to indicate that some of the components within it are Unavailable. Hover your cursor over color in the temperature bar to see the number of components that have the corresponding status.

Traffic Statistics Widget - Application Traffic Monitoring

With the Traffic statistics widget, you can monitor the live and historic statistics of devices/ objects including the number of requests being received, the load on each of the load balancers, and peak request times. The widget helps to perform an in-depth analysis of your network traffic. It will benefit traffic monitoring to track down network problems and use the information to guarantee bandwidth and quality of service for business applications.

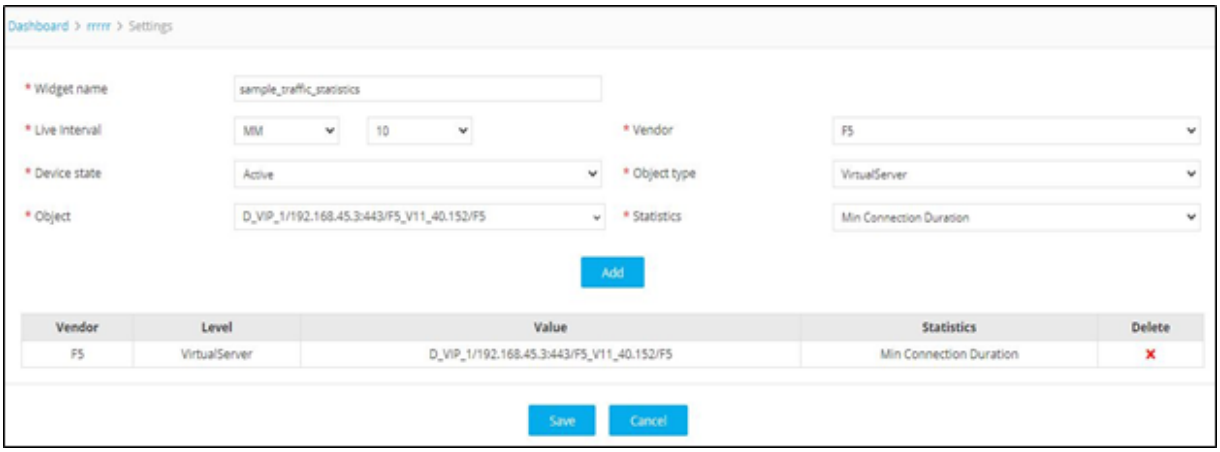
You can perform the following actions:

- Configure traffic statistics widget
- Monitor live and historic traffic flow
- Configure Traffic Statistics Widget
- Monitor Live and Historic Traffic Flow

Configure Traffic Statistics Widget

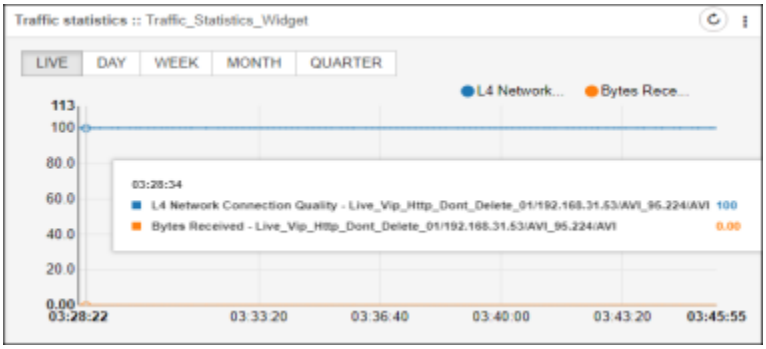
To configure a Traffic statistics widget on your dashboard,

1. If you are creating a Traffic statistics widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic above, then jump to Step 5 below. If you are creating a Traffic statistics widget for an existing dashboard, click the  (**Add widget**) button in the Command bar of the dashboard.
2. On the Create widget screen that pops up, select Traffic statistics as the widget type.
3. Enter a name for the widget.
4. Click **Create**.
5. On the Settings screen that appears, enter the time interval in minutes and seconds for collecting statistics from the devices.

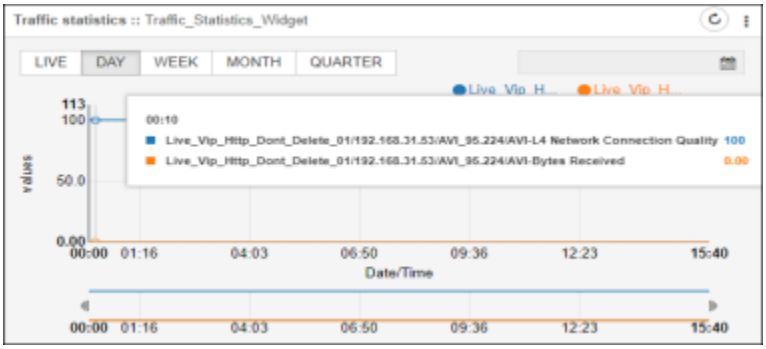


6. In the **Live Interval** field, set how often you want to collect the live performance statistics of an object.
7. In the **Vendor** field, select the vendor whose devices you want to collect statistics for A10, AVI, Citrix, or F5.
8. In the **Device state** field, select whether you want to include devices in the widget that have a status of Active, Standby, or All, where "All" means devices with a status of either Active or Standby.
9. In the **Object type** field, select the kind of object you are adding. The options that appear in this field vary depending on the vendor you selected in Step 6.
10. In the **Object** field, select an object you want to gather statistics for. The list of objects that appear varies depending on the object type you selected in Step 8.
11. In the **Statistics** field, enter the kind of statistics you want to gather. The list of statistics varies depending on the object you selected in Step 9 and can include both live and historical data within the same widget.
12. Click **Add** to add the object to the widget.

13. Repeat steps 6-11 for each vendor, device, and object you want to include in the widget.
14. When you are done adding objects, click **Save** to create the widget.
15. The dashboard screen reappears, displaying the widget (Live performance statistics) you just created.

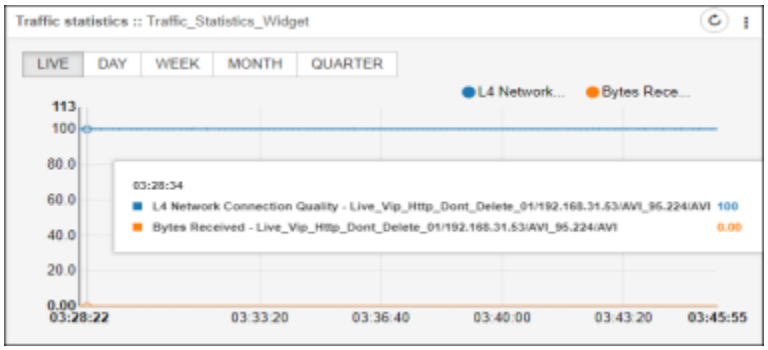


16. The historic performance statistics will be collected and displayed based on the time interval you configured in the **Settings** > **ADC** > **Statistics**. For detailed information, refer to the Statistics Settings section in the ADC Settings topic of this guide.
17. Click on Day/Week/Month/Quarter tab within the widget to view the historic performance statistics.

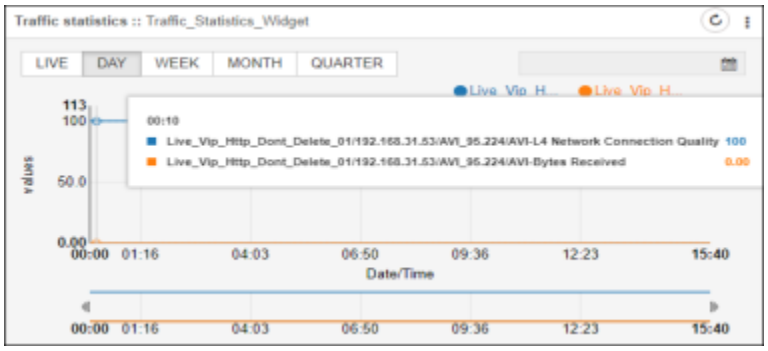


Monitor Live and Historic Traffic Flow

- The line graph represents the Live, Day, Week, Month, and Quarter data.
- The Live tab will collect the real-time statistics from the device and plot as per the interval.
- Refresh on the widget to get the latest data on-demand basis.



- The historic statistics interval should have been configured globally in the Settings menu. To configure the statistics interval, see the settings.ditamap section.
- The historical data will be collected on a regular interval, aggregated, and plotted in the form of line graphs under respective tabs.
- Click on Day/Week/Month/Quarter tab within the widget to view the historic performance statistics.
- You also have the provision to pick a date or select a range using the sliding bar and narrow it down to a particular timeline.
- Hover over the graph to get the statistics value of a particular object.



Traffic Grid Widget

With this widget, you can monitor and control the amount of application traffic that flows across the various data centers hosting the application. Rules created within the widget define what percentage of traffic goes to which data center, making it possible to maximize dispersed resources from a single location.

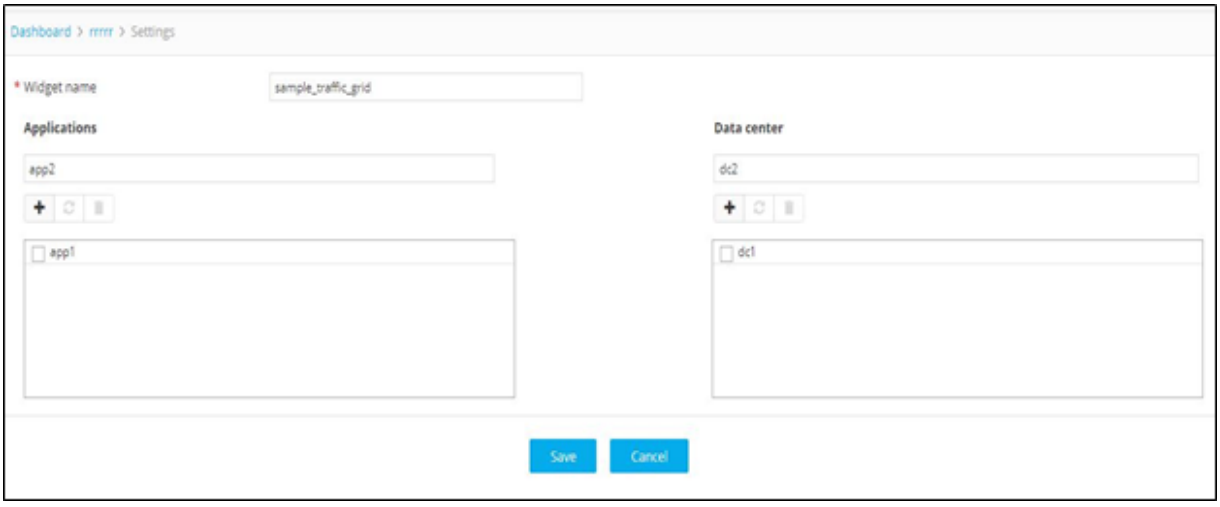
You can perform the following actions:

- Configure a traffic grid widget
- Monitor and distribute traffic across the datacenter
- Configure a Traffic Grid Widget
- Monitor and Distribute Traffic Across Datacenter
- Change the Percentage Values Within a Traffic Grid Widget

Configure a Traffic Grid Widget

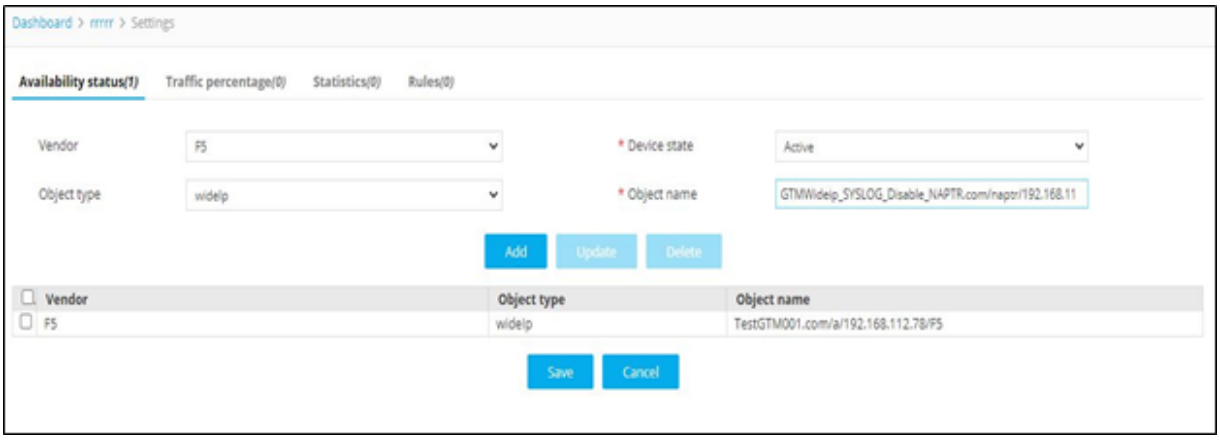
To configure a Traffic grid widget on your dashboard,

1. If you are creating a Traffic grid widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic above, then jump to Step 5 below. If you are creating a Traffic grid widget for an existing dashboard, click the + (**Add widget**) button in the Command bar of the dashboard.
2. On the Create widget screen that pops up, select the Traffic grid as the widget type.
3. Enter a name for the widget.
4. Click **Create**.
5. On the Settings screen, enter the name of the application you want to monitor traffic for.
6. Click the + (**Add**) button to add the application to the list.
7. Enter the names of the data center you want to configure traffic flows for.
8. Click the + (**Add**) button to add the data center to the list.
9. Repeat steps 5-8 for each additional application and/or data center you want to include in the widget.
10. Click **Save**.



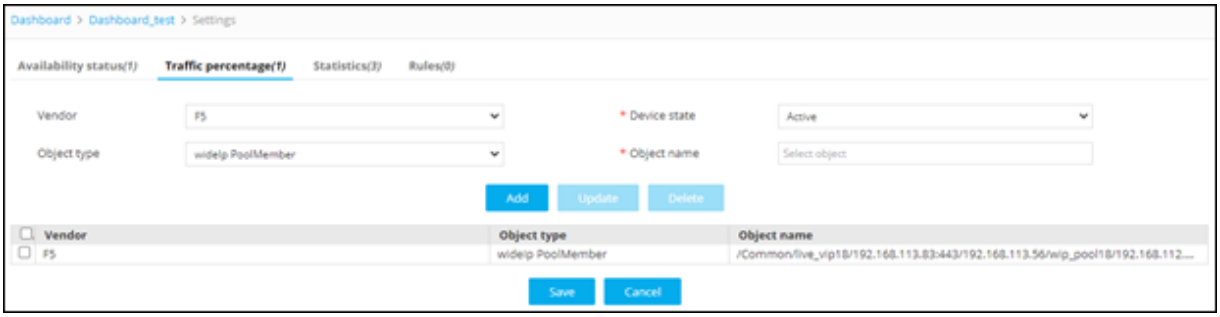
11. The widget then appears as a grid on the dashboard. Note that the applications and data centers display NA instead of statistics because they have not yet been configured.

12. Click the ⚙ (**Settings**) icon inside each Application/Datacenter cell of the grid to configure it.
13. The Settings screen appears, with the Availability status tab displayed by default.

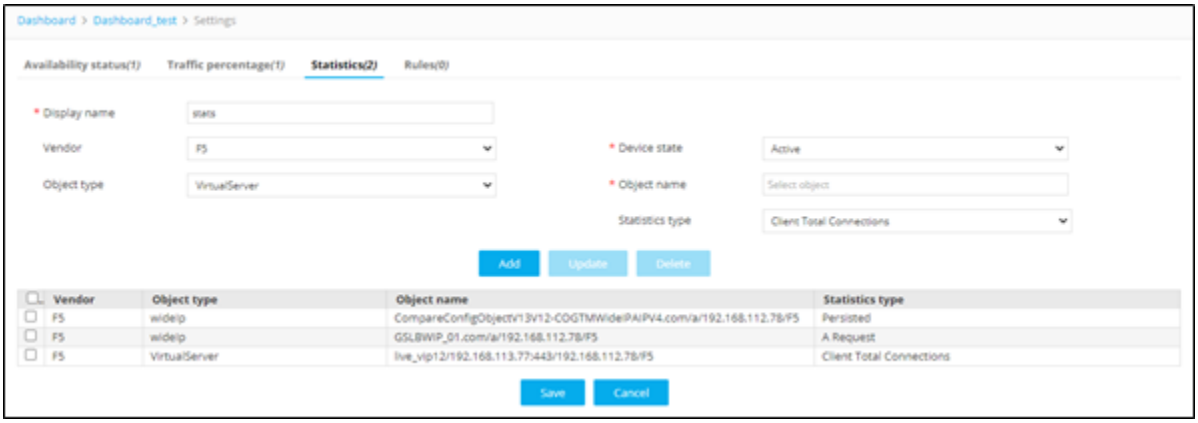


14. Select the vendor whose object you want to monitor availability in each data center.
15. In the Device state field, select whether you want to monitor the traffic for a device that has a status of Active, Standby, or All, where "All" means devices with a status of either Active or Standby. In the Object type field, select the kind of object you are adding. The options that appear in this field vary depending on the vendor you selected in Step 12. In the Object Name field, start typing to see a list of named objects whose traffic you can monitor. When you see the one you want, move your cursor over it and click it.
16. Click **Add**.
17. Repeat steps 15-16 for any other objects you want to monitor.
18. When you have finished adding all of the object types whose availability you want to monitor, click Save.

19. Click the **Traffic Percentage** tab.



20. Select the vendor whose object you want to monitor traffic across all data centers.
21. In the Device state field, select whether you want to monitor the traffic for a device that has a status of Active, Standby, or All.
22. In the Object type field, select the kind of object you are adding: wideIp Pool, wideIp PoolMember, or ItmPoolMember.
23. In the Object Name field, start typing to see a list of named objects whose traffic you can monitor. When you see the one you want, move your cursor over it and click it.
24. Click **Add**.
25. Repeat steps 23-24 for any other objects you want to monitor.
26. When you have finished adding all of the object types whose traffic percentages you want to monitor, click Save.
27. Click the **Statistics** tab.

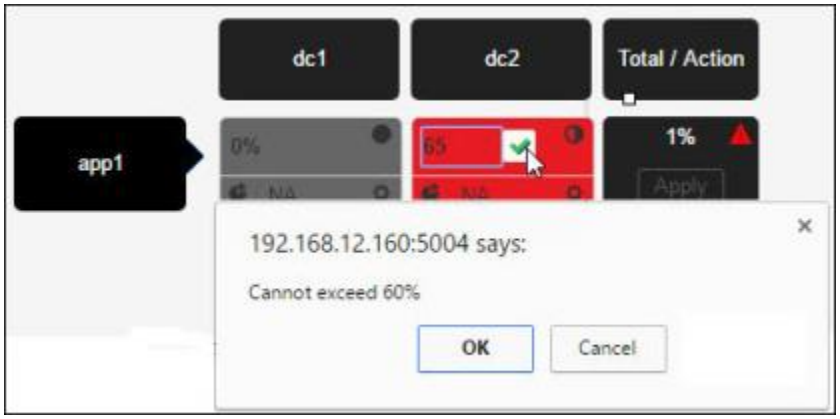


28. In the Display name field, enter the text you want to pop up when a user hovers over the (**Pie**) icon within a table cell of the widget. Note that only 10 characters can be entered in the field, so the name must be brief, but descriptive.

29. In the **Vendor** field, select the vendor whose object you want to generate statistics across all data centers.
30. In the **Device state** field, select whether you want to generate statistics for a device that has a status of Active, Standby, or All.
31. In the **Object type** field, select the kind of object you are adding: wideIp PoolMember or ItmPoolMember.
32. In the **Object Name** field, start typing to see a list of named objects whose statistics you can generate. When you see the one you want, move your cursor over it and click it.
33. Click **Add**.
34. Repeat steps 32-33 for any other objects you want to generate statistics for.
35. Click **Save**.
36. Click the **Rules** tab if you want to create rules that govern traffic percentages for the widget.

37. In the **Rule type** field, select one of the following options:

Note: Warning - A warning rule causes a popup text box to appear if the user violates the restrictions defined by the rule, but the user can still complete the action. For example, if you create a rule that says a data center cannot receive more than 60% of the traffic on a device and a user tries to set the percentage for that data center to 65%, a warning pops up on the screen when the user clicks the (Enter) icon in the table cell, as shown below. Despite the warning, the value 65 remains in the cell after the user closes the popup screen.

- 

  Restriction - A restriction rule causes a popup text box to appear if the user violates the restrictions defined by the rule. In this case, the user is unable to complete the action. For example, if you create a rule that says a data center cannot receive more than 60% of the traffic on a device and a user tries to set the percentage for that data center to 65%, a restriction screen pops up on the screen when the user clicks the (Enter) icon in the table cell. When the user clicks OK to dismiss the popup, the percentage in the cell automatically reverts to its original value, erasing the user's entry of 65%.

- **Action** - An action rule causes an event that you define to happen when the traffic percentage for a data center reaches a level or range that you define. The two main event types are Enable and Disable, so when the level you set is reached, an object or set of objects you selected is automatically enabled or disabled.

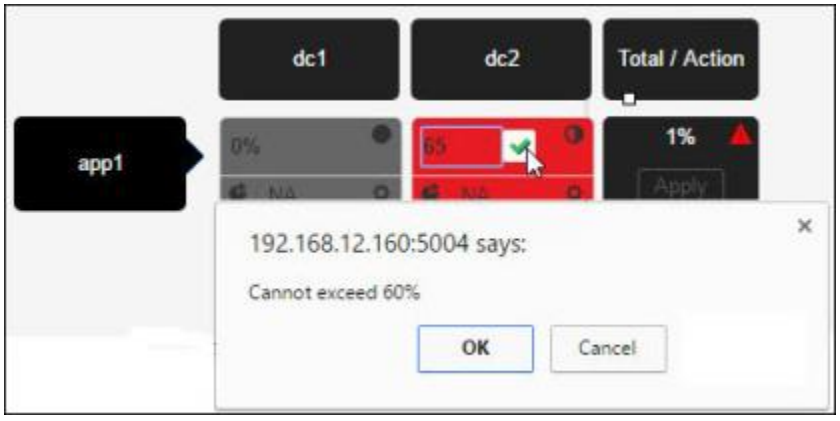
38. When you are finished creating rules for the widget, click **Save**.
    For instructions on how to change the percentage values within the Traffic grid widget cells, refer to Change the Percentage Values Within a Traffic Grid Widget.

Monitor and Distribute Traffic Across Datacenter

- The availability status (Up/Down/Offline etc.,) of the Application will be represented in appropriate color code along with the statistics value that is configured.
- The current Traffic percentage can be reviewed and distributed to other data centers accordingly. Distribute the traffic that equals to 100% and click Apply.
- Applying the changes will modify the ratio of the members on the end device.
- If the traffic percentage applied is not successful, the user will be indicated with a red triangle alert icon against the applications.

- During Maintenance, if a particular data center should not be receiving any traffic, it can be made 0 and the rest of the data centers can distribute the load.
- The traffic distributions are always reflected on current active devices.

- If a Rule is configured, before executing the traffic percentage changes, the rule condition will be validated.
  - In case of a Warning rule, the end-user will be prompted with a warning message to not proceed. Users can choose to Terminate or proceed with the changes.
  - In case of a Restriction rule, the end-user will not be able to proceed with the changes on exceeding the threshold limit.
  - When an Action rule is configured and if the traffic percentage meets the condition, the configured objects will be automatically Enabled/Disabled accordingly.



Change the Percentage Values Within a Traffic Grid Widget

To change the traffic percentages listed for each data center in a Traffic Grid widget, complete the following steps:

1. Open the dashboard containing the Traffic Grid widget you want to update.
2. Click the current percentage value for the first data center.
3. The cell then becomes a text-entry field, as shown in the bottom-right cell in the image below.

4. Enter the new percentage in the text field.
5. Click the (**Enter**) icon to save your changes.
6. Repeat the process for each of the other data centers, ensuring that the total equals 100%.
   For an explanation of the different colors and symbols displayed in the cells, refer to View the Different Statuses and States for a Widget for a Widget.

Script Execution (SE) Widget

A Script execution widget saves script files on a local machine and provides easy access to maintain and execute script commands from within the widget. The script files (shell or python) are pre-written files existing in the AppViewX server. It allows the user to enable/disable actions that are performed through the action widgets and also, to write custom scripts that can be remotely run on the ADC devices.

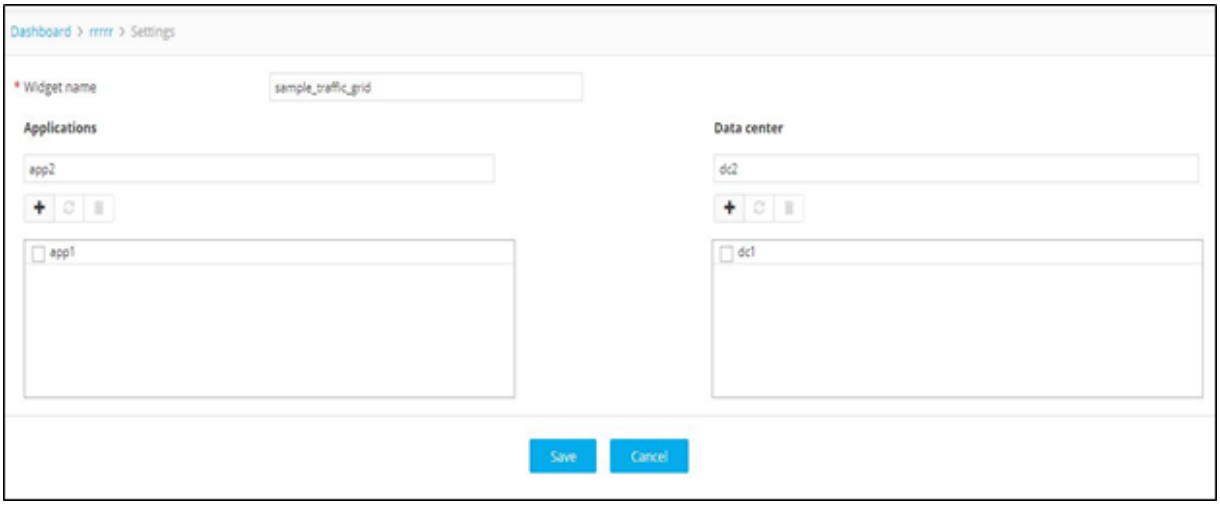
You can perform the following actions on the widget:

- Configure a script execution widget
- Execution of script
- Configure a Script Execution Widget
- Execution of Scripts

Configure a Script Execution Widget

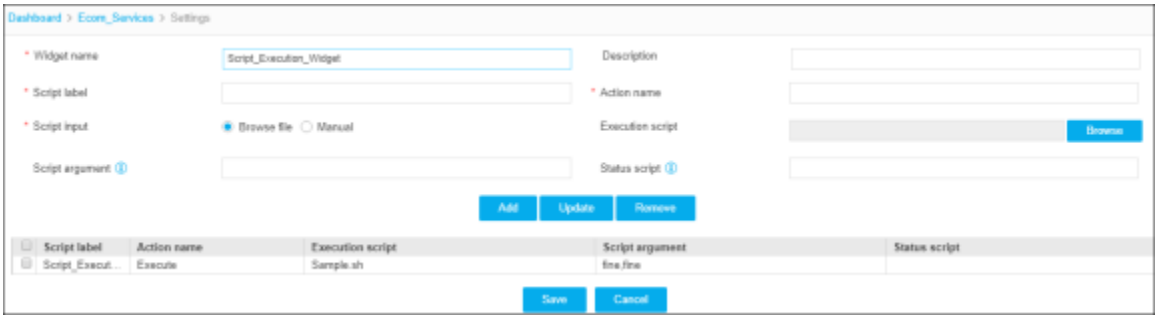
To configure a Script execution widget on your dashboard,

1. If you are creating a Script execution widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic above, then jump to Step 5 below. If you are creating a Script execution widget for an existing dashboard, click the  (**Add widget**) button in the Command bar of the dashboard.
2. On the **Create widget** screen that pops up, select **Script execution** as the widget type.
3. Enter a name for the widget.
4. Click **Create**.
5. On the **Settings** screen that appears, enter a description of what the script does so that it can be readily identified when viewed through the widget.



6. Enter a label for the script bar you will be adding to the widget. The **Label** should help identify what sort of script you are adding so that it can be readily identified when viewed through the widget.
7. In the **Action Name** field, enter the action that you want to perform using the script execution widget.
8. Select the **Browse file** or **Manual** radio button based on how you want to upload the scripts.
9. In the **Execution script** field, do the following:
   - If the *Browse file* radio button is selected in Step 8, click the **Browse** button and navigate to the file you want to add, then click **Open**.
   - If *Manual* is selected in Step 8, enter the full path of the script. These scripts will need manual intervention to execute.
10. In the **Script argument** field, enter any information for the script with a comma as delimiters. Upon script execution, the mentioned arguments are passed to the script provided that the script is capable of receiving arguments (through variables).
11. (Optional) In the **Status script** field, enter the full path of the script to update the color and status message of the bar. The status and result of the script are updated simply by loading or refreshing the widget.

12. Click **Add** to add the details in the table at the bottom of the screen.

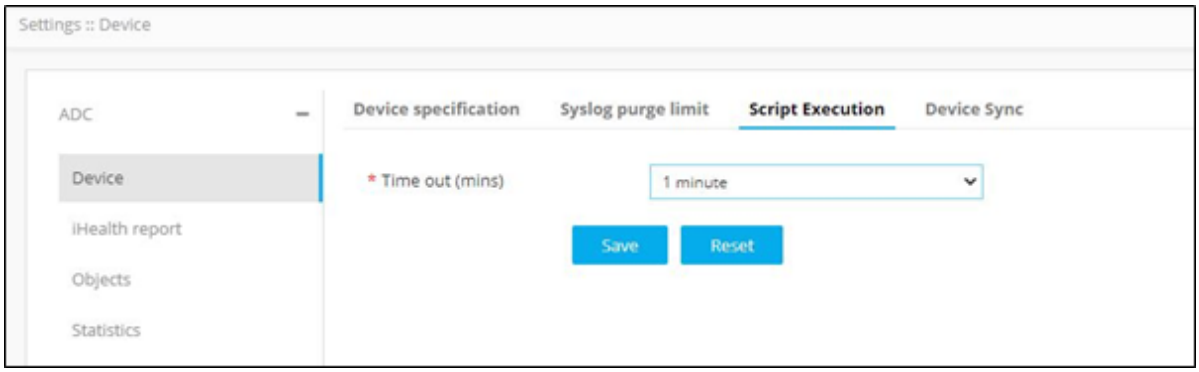


13. Repeat steps 5-12 for each additional script you want to add.
14. Select the checkbox beside the script label column and then, click Save.
15. Configure script timeout to avoid prolonged script execution. To configure the script timeout,

    • Go to ☰ **Menu** > **Settings** > **ADC** > **Device** > **Script Execution** > **Time out**.

    • Mention the time out from 60 seconds to 5 minutes. The default timeout is 60 seconds (1 min).

> **Note:** For more detail, see Script Execution in the Device_Settings.ditamap.

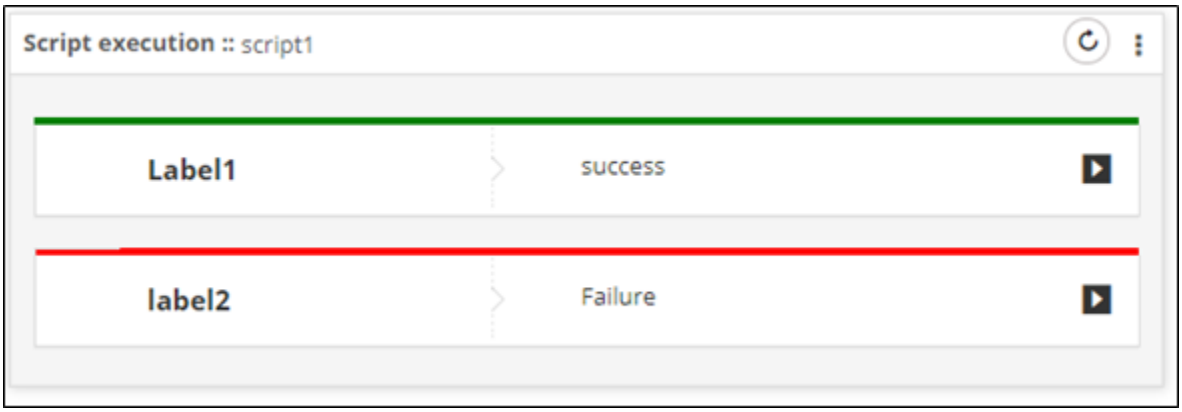


Execution of Scripts

On the successful configuration of widget for script execution, the scripts can be executed on a need basis.

To execute the script,

1. Click (**Play**) on the widget.



2. The color and message on the bar is determined by the following return message of the status script:

echo Color:Green,Response:"Pool failover_pool_web is up"
Color: Green - to update the color of the bar to green
Response:"Pool failover_pool_web is up" - to show the string inside "" as status
Color: Red - to update the color of the bar to red

3. The status script will update or run on every refresh of the widget, to get the latest status.

> **Note:** Frequent use cases like Device Memory check, CPU check, etc., can be executed quickly on demand, which will provide the run time data from the device.

4. To run the execution script, click the Play button and select one of the following:
   - **Action name**: To internally trigger the execution from the AppViewX server CLI.
   - **View Logs**: To check the previous logs of the script that are executed.
5. When it finishes, a popup screen appears listing the script execution logs, as shown in the following example:

6. Click the **Download file** button if you want to download an output file.
7. The file is downloaded to your computer.
8. Navigate to the location where you want the file to go, then click **Save**.

Class Management Widget

A Class management widget allows you to view and modify the classes associated with iRules for devices. By grouping objects into classes and assigning actions to the classes, users are able to configure ADC devices within AppViewX. There is no need to access the ADC devices directly, which eliminates the chance of crashing a box with syntactically incorrect commands.

iRule is a flexible feature that lets the user manage or customize their application traffic. Classes are usually defined within an iRule. String, Address, Integer are different kinds of classes. The following section explains data group/classes and their types.

Data Group/Classes

A data group is a simple group of related elements like a set of IP addresses of a class.

Data groups can be one of the following types:

- **Address**: An address data group consists of a collection of IP addresses.
- **String**: A string address group consists of a group of strings, such as *.jpg.
- **Integer**: An integer data group consists of a group of integers.
- **External File**: You have the option to store data groups in an external file. The benefit of storing data groups in an external file is the data does not need to be sorted by the system when it is loaded

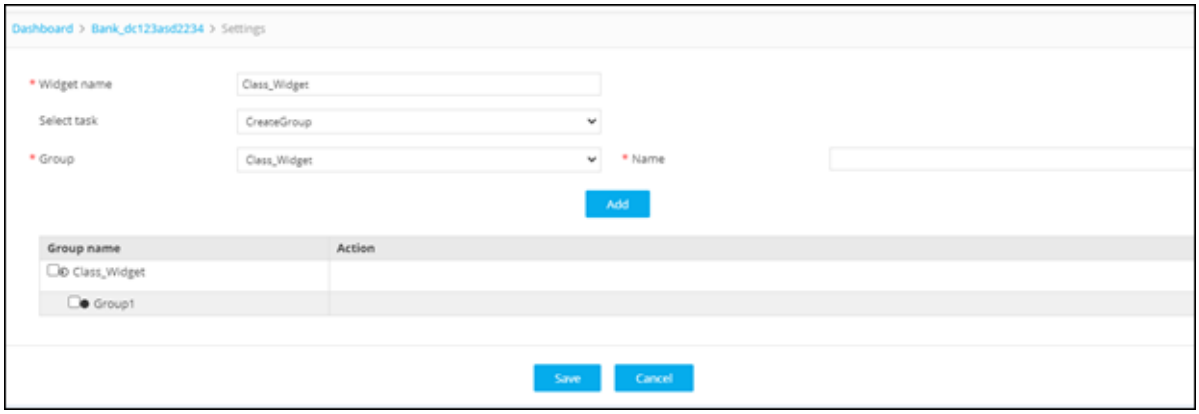
because it is stored outside of the **bigip.conf** file. The elements in the external data group file should be stored in comma-separated lists with a newline character after each entry. Refer to the *BIG-IP Configuration Guide* for more details about Data Groups.

- Configure a Class Management Widget

Configure a Class Management Widget

To configure a Class management widget on your dashboard,

1. If you are creating a Class management widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic above, then jump to Step 5 below. If you are creating a Class management widget for an existing dashboard, click the  (**Add widget**) button in the Command bar of the dashboard.
2. On the **Create widget** screen that pops up, select Class management as the widget type.
3. Enter a unique name for the widget.
4. Click **Create**.
5. On the Settings screen, configure Actions to any of the following as per the need:
   - **View class** - to configure view class, see Configure View Class section.
   - **Modify class** - to configure modify class, see Configure Modify Class section.



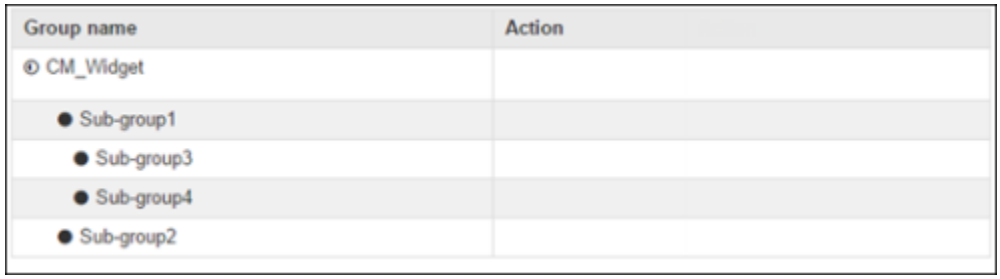
- Configure View Class (Internal/External)
- Configure Modify Class (Internal/External)

Configure View Class (Internal/External)

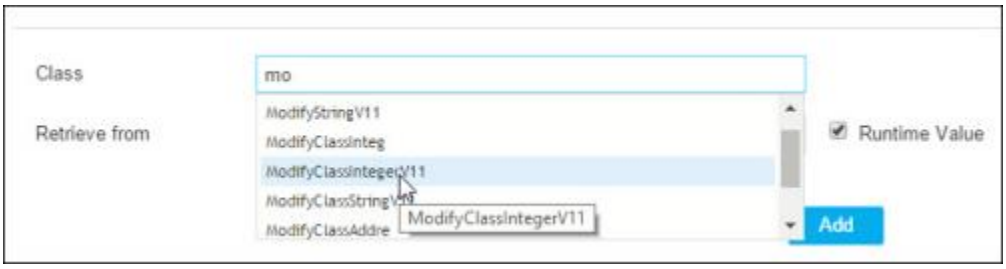
View class action retrieves the configured class attributes from the device and allows to view the latest configuration.

To create a view class,

1. Leave the Select task field set to CreateGroup.The Group field automatically uses the widget name as the default group.
2. Enter a name for the group.
3. Click Add to add the group to the widget.
4. (Optional) If you want to create a sub-group, enter another group name in the Name field and click Add. The new group is added under the original one.
5. (Optional) If you want to create a sub-group of a sub-group, select the sub-group in the Group dropdown list, then enter the sub-sub-group name in the Name field before clicking Add.
6. In the example below, CM_Widget is the group, Sub-group1 and Sub-group2 are created as sub-groups of CM_Widget, and Sub-group3 and Sub-group4 are created as sub-groups of Sub-group1.

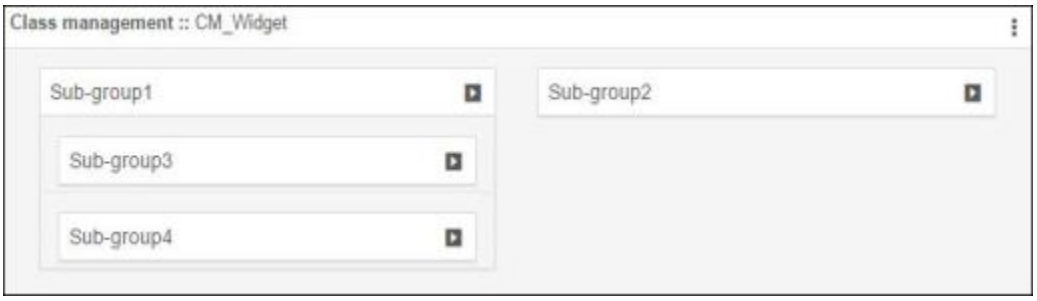


7. After you have finished creating groups and sub-groups, select CreateAction from the Select task dropdown menu.
8. The screen refreshes to display new fields on the screen.
9. In the **Actions** field, select **View Class**.
10. In the **Group** field, select the group you are creating the action for.
11. In the **Name** field, give the action a name that clearly identifies what action the user can take.
12. In the **Class** field, start typing the name of the class that you are creating a view or modify action for. As you start to type, all classes that match the characters you have entered so far appear in a list. Select the class you want to add.



Note: For F5 devices, the classes are controlled by the permission provided in the Resource section. Based on the permission given for the classes, they appear in the **Class** field dropdown list for the selection. If no permission has been given for the classes, they do not appear in the **Class** field dropdown list. In case the permission has been removed for the classes while you manage a class in the dashboard, the "Permission Denied" notification will be displayed.

13. The Retrieve from field populates automatically with the location of the class that you selected in Step 15.
14. Enabling the Run time value option, allows the end-user/consumer to change the class name during the execution.
15. Click Add to add the class to the group.
16. The group and all sub-groups you just created appear in a hierarchical structure within the widget.
17. Click the ▶ (**Actions**) icon to access the list of available actions for the corresponding group or sub-group.



Note: If needed modify the configured Group/Action.

Configure Modify Class (Internal/External)

Modifying class action allows you to view and change the details of a class.

To create a modify class,

1. Leave the **Select task** field set to CreateGroup.The Group field automatically uses the widget name as the default group.
2. Enter a name for the group.
3. Click **Add** to add the group to the widget.
4. (Optional) If you want to create a sub-group, enter another group name in the Name field and click Add. The new group is added under the original one.

Heatmap Widget

A Heatmap widget allows you to view statistics for managed, failed, and unresolved devices or device groups. Widget will collect the statistical data for Inprogress, queued, failed, and managed devices as long as the objects are available in the database. The heatmap reports are not viewed for unmanaged devices.

In the Heatmap widget, ADC device groups appear as color-coded blocks, with the colors representing the following:

- **Green** - All devices in the group are healthy
- **Red** - At least one device in the group is in a critical state
- **Gray** - Statistics have not been collected for the device group.
- **Orange** - One or more devices in the group have reached a warning limit

Copy a Widget to Another Dashboard

To copy a widget to another 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 containing the widget that you want to copy.
3. Click the (**Options**) button and select the (**Copy to**) icon in the Command bar at the top of the widget.
4. On the Copy widget screen that pops up, select the dashboard you want to copy the widget.
5. Click **Copy to Finish**.

Move a Widget to Another Dashboard

To move a widget to another 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 containing the widget that you want to move.
3. Click the (**Options**) button and select the (**Move to**) icon in the Command bar at the top of the widget.
4. On the Move widget screen that pops up, select the dashboard you want to move the widget to.
5. Click **Move to Finish**.

Delete a Widget

Deleting a widget removes it from the current dashboard, but does not remove it from any other dashboards it has been copied to.

To delete a widget, complete the following steps:

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 containing the widget you want to delete.
3. Click the (**Options**) button and select the (**Delete**) icon in the Command bar of the widget.
4. On the confirmation screen that pops up, click **Yes**.
5. The dashboard refreshes and no longer displays the widget.

Custom Widget

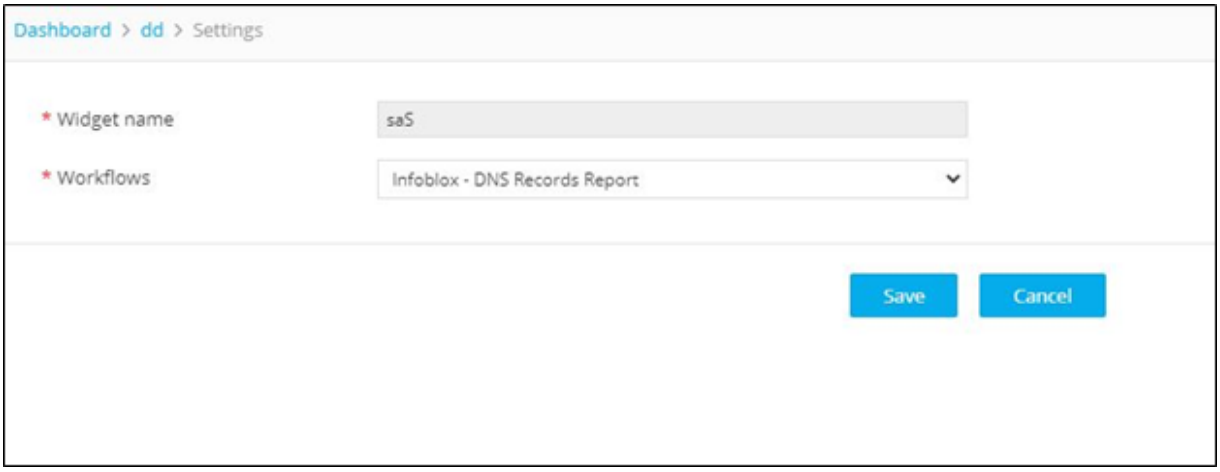
Custom reports are used for monitoring the usage of the device and application metrics, which are configured by existing workflows.

- Configure a Custom Widget Using Workflow

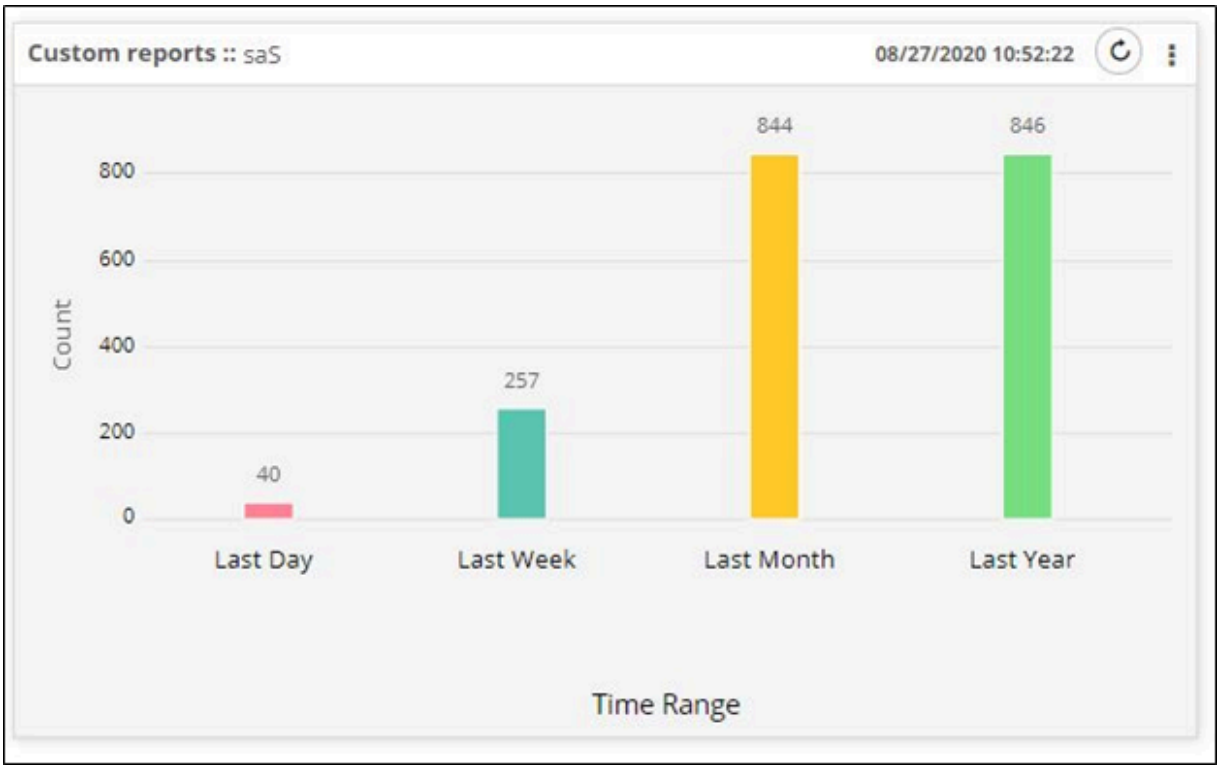
Configure a Custom Widget Using Workflow

To configure a customreports widget on your dashboard,

1. In the Dashboard, click the (**Add widget**) button in the Command bar of the dashboard.
2. On the **Create** widget screen that pops up, select **Custom reports** as the widget type.
3. Enter a name for the widget, and then click **Create**.
4. Custom reports configuration screen appears.



5. In the **Workflows** field, select the workflow that you want to monitor the usage of the device and application metrics.
6. When you are done configuring the Custom reports settings, click **Save**.
7. The custom reports widget is displayed on the dashboard, with configured workflow reports.



Studio Based Reports

The Reports sub-system within the Studio module allows you to perform the following tasks:

Note: For more details about the report, refer to the Reporting User Guide.

- Clone a Report
- Create a Report
- Delete a Report

Clone a Report

To clone a report,

1. Click **Menu** > **Studio** > **Reports**.
   The Reports screen appears.

2. In the **My Reports** tab, all the reports are displayed based on the permissions that you have been assigned. Select the report you want to clone.
3. From the **Actions** dropdown, click **Clone**.
4. In the **Clone report** screen that appears, enter a **Name** for the cloned report.
5. Click **Save**.

Create a Report

To create a report using the Reports sub-system in the Studio module,

1. Click **Menu** > **Studio** > **Reports**.
2. The **Reports** screen appears. In the **My Reports** tab, all the reports are displayed based on the permissions that you have been assigned.
3. Click **Create New Report**.
4. In the **BASIC INFO** screen of the report creation wizard,
   - Enter a **Name** for your report.
   - (Optional) In the **Description** field, type additional information related to the report.
   - Click **Yes** if you want to control access to the report using different permissions for different users.
   - Click **Save** to resume the chart creation later or click **Next** to proceed with the chart creation.
5. In the **DATA SOURCE** screen,
   - From the **Select data source** dropdown, choose one of the following sources to query data, and build the report:
     - **Query builder** - Allows you to select one of the existing queries or create a new query.
     - **Hooks** - Allows you to select one of the pre-built OOB hooks or create a new hook (Script or REST).
   - Click **Save** resume the chart creation later or click Next to proceed with the chart creation.
6. In the **CHART CONFIGURATION** screen,
   - Click on one of the following reports to **Select chart type - PIE**, **DONUT**, **BAR**, **STACKED BAR**, **GRID**, **LINE**, and **METRIC**.
   - The fields that appear vary for each chart type, at a minimum, fill in all the mandatory fields.
   - Click **Save** to resume the chart creation later or click **Next** to proceed with the chart creation.
7. In the **CHART DRILLDOWN** screen, select the checkbox to view more specific layers of the data or information being analyzed.

8. Select one of the following drill-down types for the chart:
   - **Set redirect URL** to configure the URL to any page to which the redirection from the chart must happen.
   - **Grid** to associate the chart to a hook and a workflow.
9. Click **Save & Enable** to save the report to the AppViewX system.
10. The report is added to the **My reports** tab, it can be enabled or disabled using the toggle button in the **Status** column.
11. After the report is created, you can perform one of the following actions on the left-hand pane:
    - **Pin** the report to a new or an existing dashboard.
    - Set the **Interval** during which the chart data must be collected. This can be customized to happen once or recursively.
    - **Share** the report with the various recipients at a specific point of time once or repeatedly.
    - Enable or disable the report using the toggle button.

Delete a Report

To delete one or more reports,

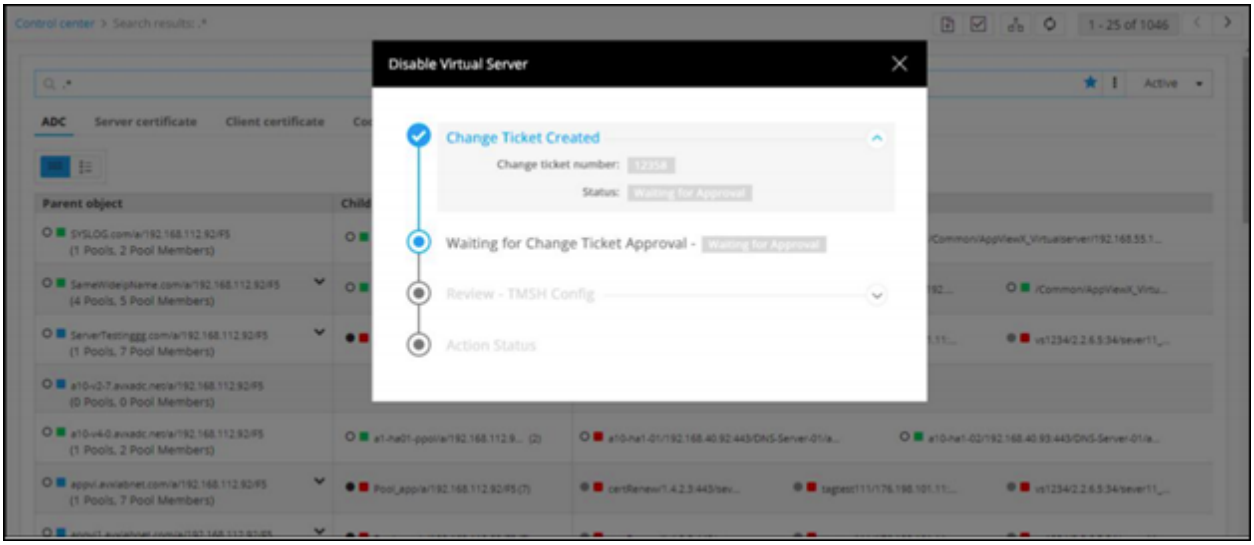
1. Click **Menu** > **Studio** > **Reports**.
   The **Reports** screen appears.

   In the **My Reports** tab, all the reports are displayed based on the permissions that you have been assigned.
2. Select the report(s) you want to delete.
3. From the **Actions** dropdown, click **Delete**.
4. In the **Confirm delete** dialog box that appears, click **Yes**.

Launch Automation from Application-Centric View through Rules

- Enforce business process and launch automation from App-centric views through the Rule configuration.
- Actions that are triggered from App-centric views will look for Rules configured and execute an appropriate workflow in the background.

- Upon executing any action, a request ID will be generated and a stage view will be displayed representing the action status.
- The request ID could be used to track progress at any point in time.
- Sample use cases
  - Service NOW integration for any action triggered from AppViewX.
  - Prevent users from taking all servers out of rotation as this might lead to an application-level outage.
  - Email notification for any Server Rotation action performed by the team member.



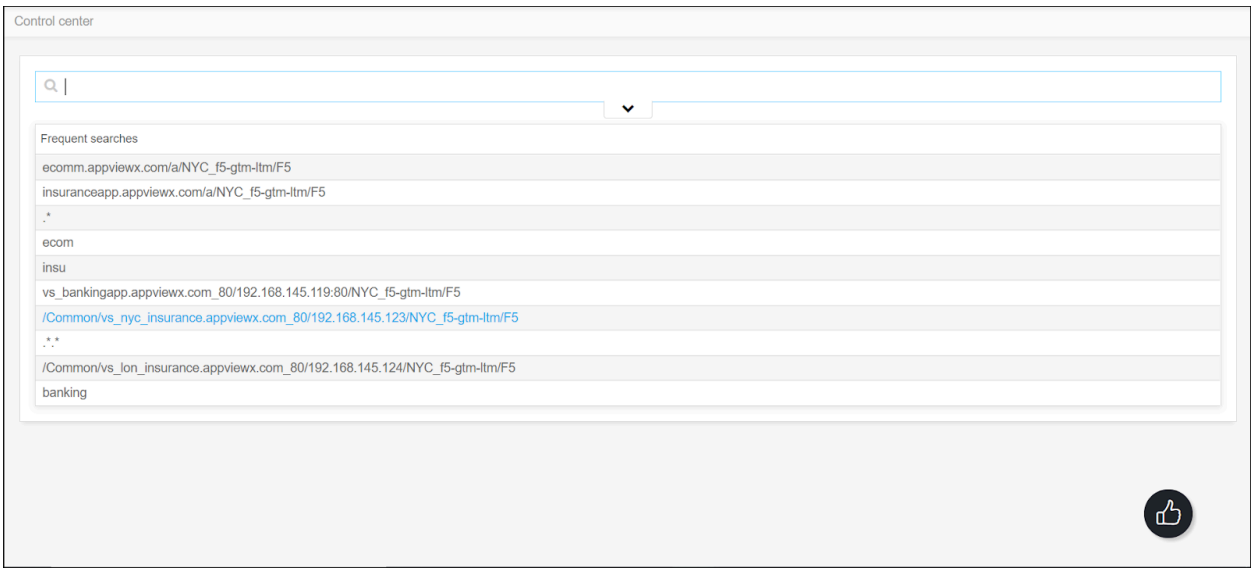
App Search

- App Search - Overview
- Run a Search
- Create a Bookmark
- View Basic Details of ADC Search Results
- View Additional Details of Search Results
- Filter ADC Search Results
- Export Search Results
- Access the Actions Menu for Objects on the ADC Search Results and Topology Screens
- Compare ADC Objects

- Filter the Information Displayed in an ADC Topology
- View Configuration Details
- View Timeline Statistics for an Object

App Search - Overview

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.

Run a Search

To run a search within the Control Center,

1. Click **Menu** > **ADC+** > **App Search**.
2. In the App Search module, the Control Center search screen is displayed by default. The ways to search the ADC devices are:

- Search Using Free Text Entries
- Search Using Frequent Search Links
- Search Using Predefined Search Keys
- Search Using Regular Expression (Regex)

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 Citrix would be **citrix_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:

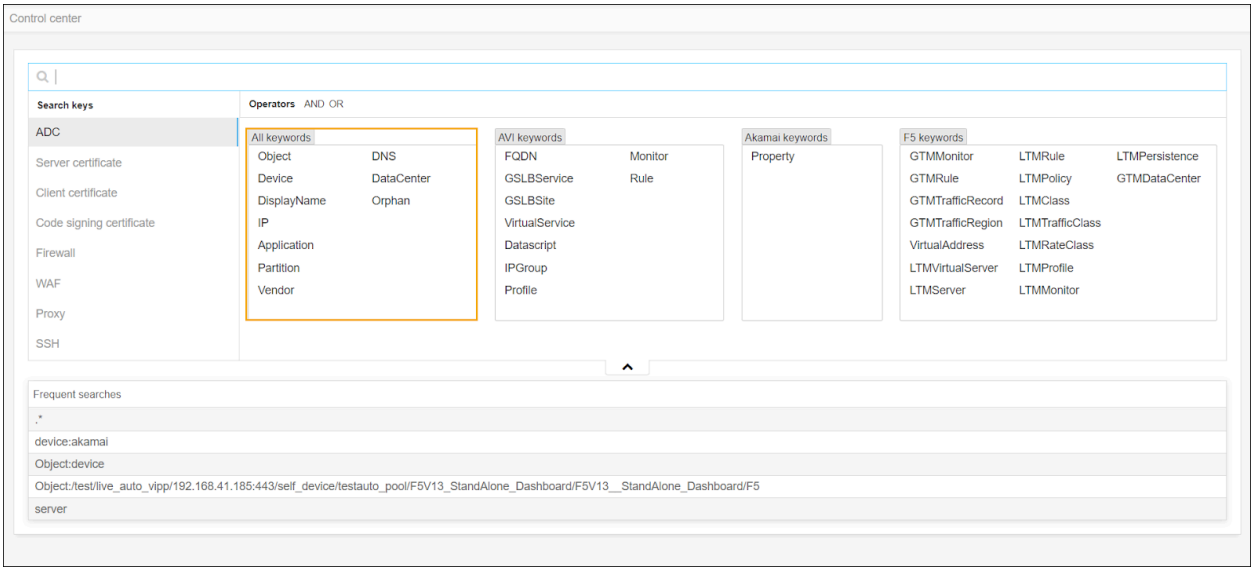
- All keywords
- Vendor-specific keywords
- Logical operator with keywords

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
- Vendor-Specific Keywords
- Logical Operator with Keywords
- 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>

Common Keywords	Description
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. 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, Citrix, 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.

• Sample Search Keywords

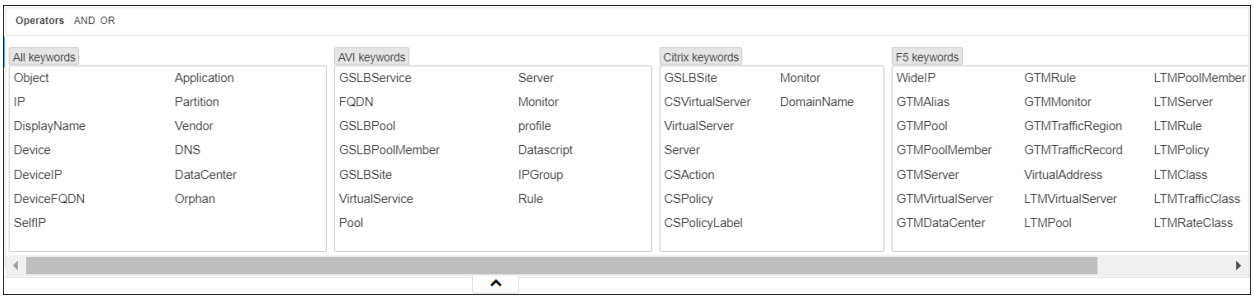
Sample Search Keywords

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.

Common Keywords	Description
	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. 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, Citrix, 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.

Vendor-Specific Keywords

ADC vendor-specific keywords are available to search for objects from a particular ADC vendor. The keywords are grouped as per the vendors managed in the inventory.



Sample Search Queries

Vendor-Specific Keywords	Description

vendor:Citrix AND CSVirtualServer:.*	The list of all the CS Virtual Server applications from Citrix devices managed in AppViewX.
vendor:Citrix AND CSVirtualServer:Test.*	The list of all the CS Virtual Server applications from Citrix devices containing Test in it.
vendor:AVI AND FQDN:.*	The list of all the applications with FQDN from all the AVI devices managed into AppViewX.
vendor:AVI AND FQDN:Test.*	The list of applications with FQDN containing “Test” in it, from all the AVI devices managed into AppViewX.

• Sample Search Queries

Sample Search Queries

Vendor-Specific Keywords	Description
vendor:Citrix AND CSVirtualServer:.*	The list of all the CS Virtual Server applications from Citrix devices managed in AppViewX.
vendor:Citrix AND CSVirtualServer:Test.*	The list of all the CS Virtual Server applications from Citrix devices containing Test in it.
vendor:AVI AND FQDN:.*	The list of all the applications with FQDN from all the AVI devices managed into AppViewX.
vendor:AVI AND FQDN:Test.*	The list of applications with FQDN containing “Test” in it, from all the AVI devices managed into AppViewX.

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.

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.

Search Using Regular Expression (Regex)

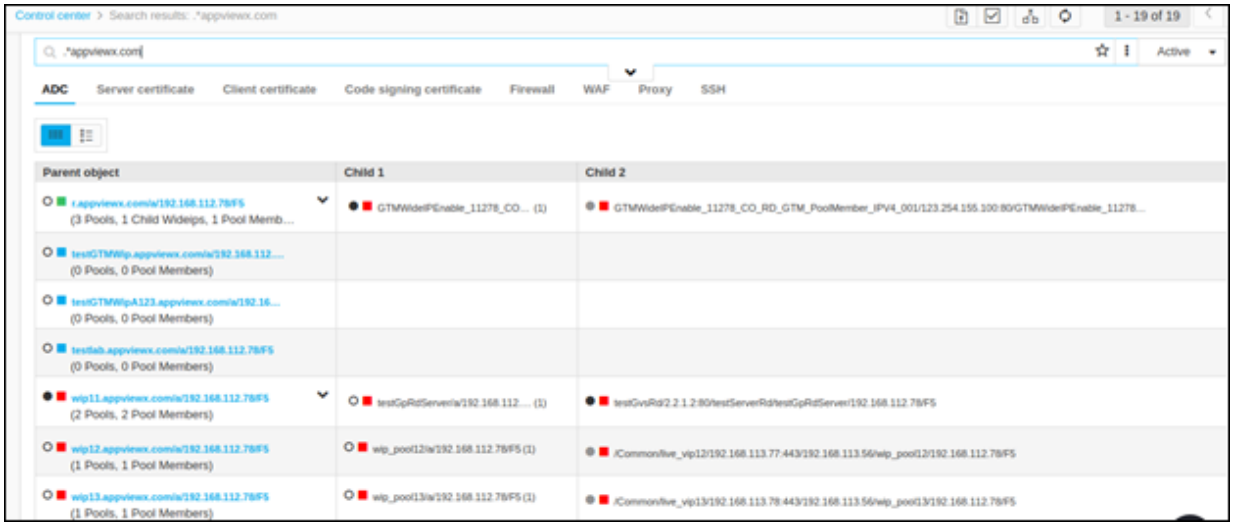
You can enter regex (such as * or .*) or the object/certificate name followed by the regex (.*) in the search field and click Enter on your keyboard. The search results will be displayed as follows:

- .* - All the device objects/certificates along with their hierarchy are displayed in their respective tabs.
- (searchstring).*- This RegEx results in the objects, whose name starts with the search string..
- The search results that are matched with the text entered will be highlighted.

Examples

• For the RegEx **gs-f5-pe.***, the search results that are matched with the text entered will be highlighted:

• If all the subdomains of a DNS are needed to be searched, then .*DNSName shows all the subdomain:



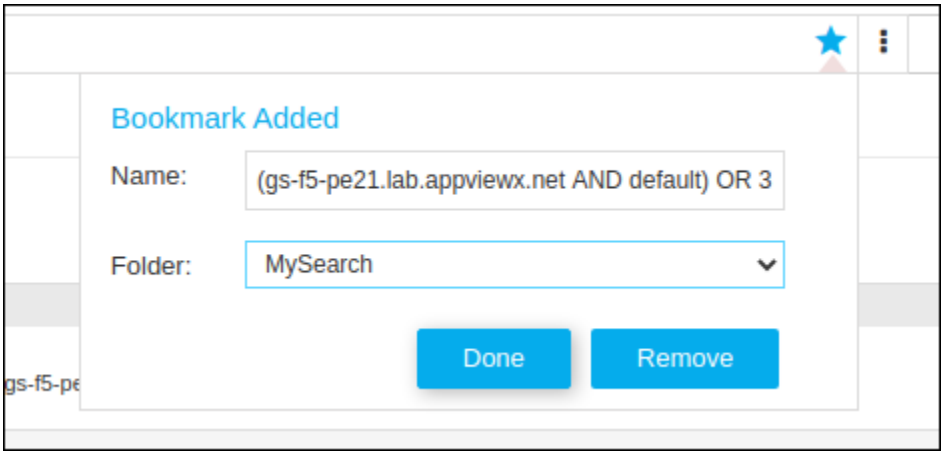
Create a Bookmark

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.

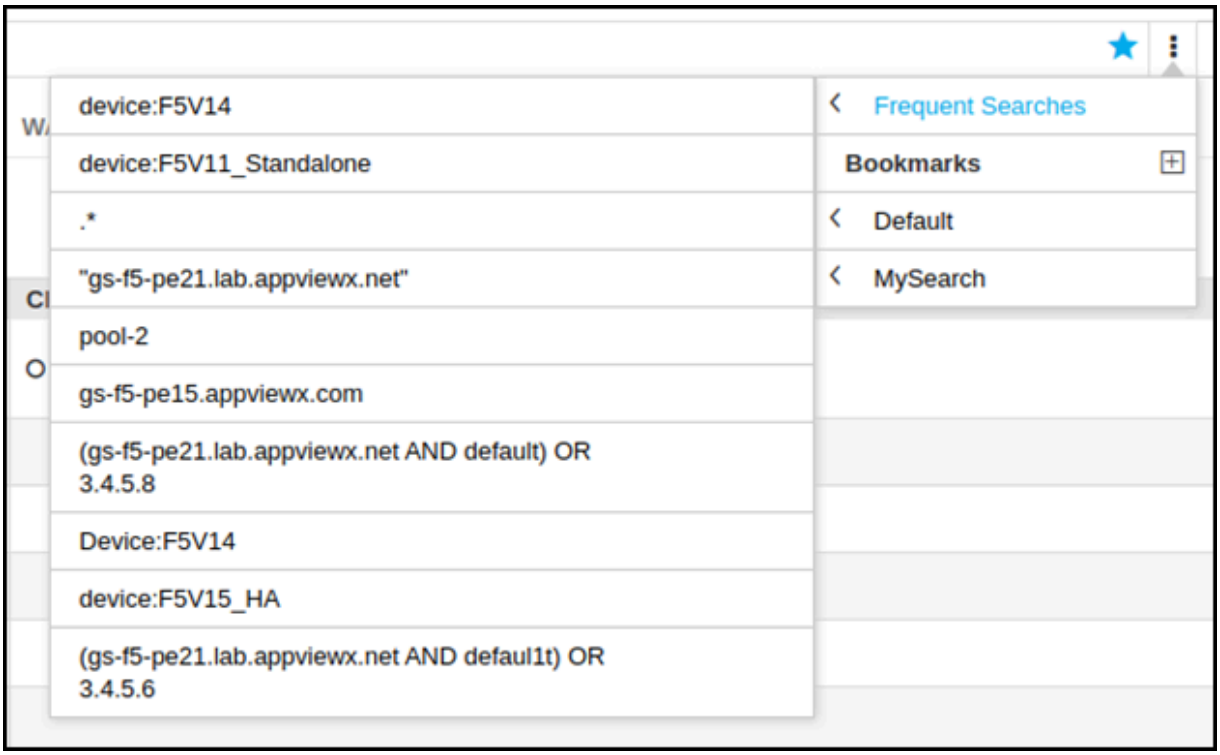
4. Click the button to create a bookmark folder.
5. Click the button on the search bar. A pop-up message will be displayed at the top of the screen, **Bookmark(s) created successfully**.
6. On the **Bookmark Added** pop-up screen, enter a name for the bookmark to help the users identify it.



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:



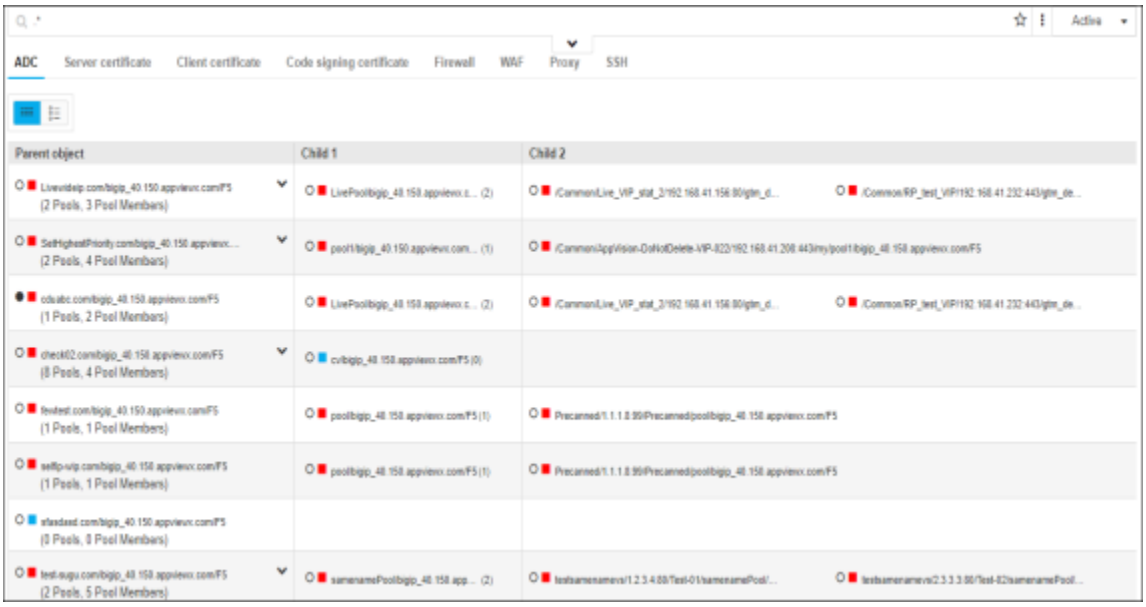
View Basic Details of ADC Search Results

In the App Search module, the Control Center is designed to display the ADC search results in both the Application and Infrastructure View. Although each view displays the search results in a different manner, the same search query is used. In order to view the search results, ensure that you have been assigned to a role that has access to Application View and/or Infrastructure View along with the set of actions you want to perform on the objects.

- Application View
- Infrastructure View

Application View

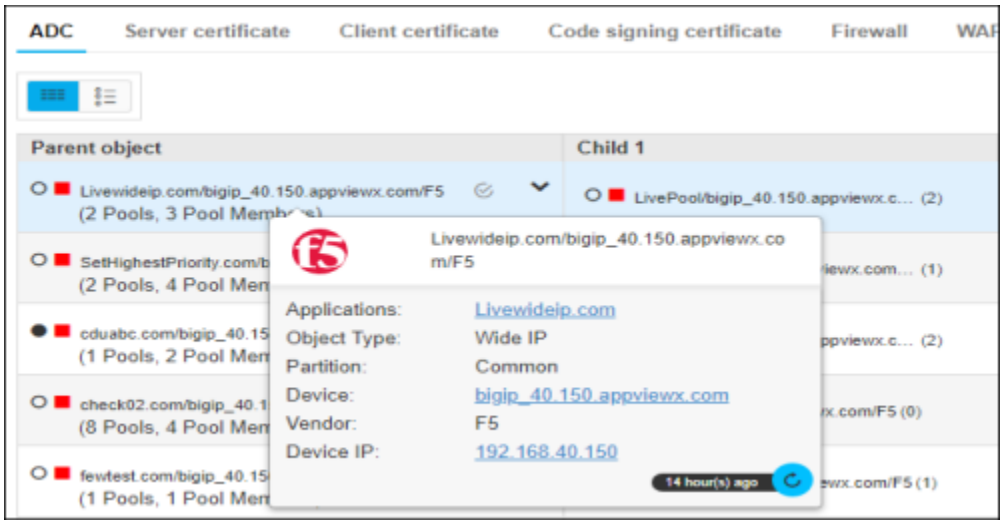
This is the default search result landing page. The parent objects are listed in the left-most column and related first-level children and second-level children appearing in subsequent columns.



To view the basic details of search results within the Control Center,

1. Run a search.
   By default, search results are displayed in the Application view.
2. Each object has a series of symbols that appear before its name. You can hover over the icon to identify the State/Status of the objects.
   - **Circles (State)**
     - ● A solid black circle indicates that the object is disabled
     - ○ A hollow circle indicates that it is enabled
     - ● A solid grey circle indicates that the object is parent disabled
   - **Squares (Status)**
     - ■ A green square indicates that the object is available and enabled
     - ■ A blue square indicates that the object is unknown and disabled
     - ■ A red square indicates that the object is offline and enabled
     - ■ An orange square indicates that the object is offline but might become available again and enabled.
   - Get additional information about the object on hovering. An actionable tooltip will be available that represents the object's details, last refresh time, etc.
   - In the search results field, hover your cursor over the result whose basic details you want to view.

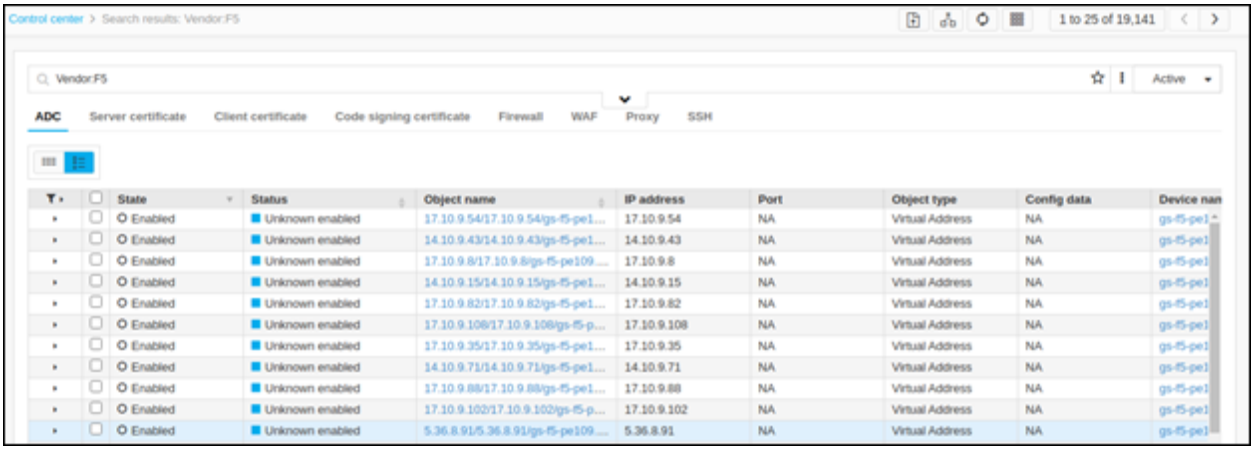
- A popup box appears, listing the details for the object.



- The DNS name of an object (applicable only for F5 device objects) will be displayed in the pop-up box only if DNS is configured during AppViewX installation.

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.

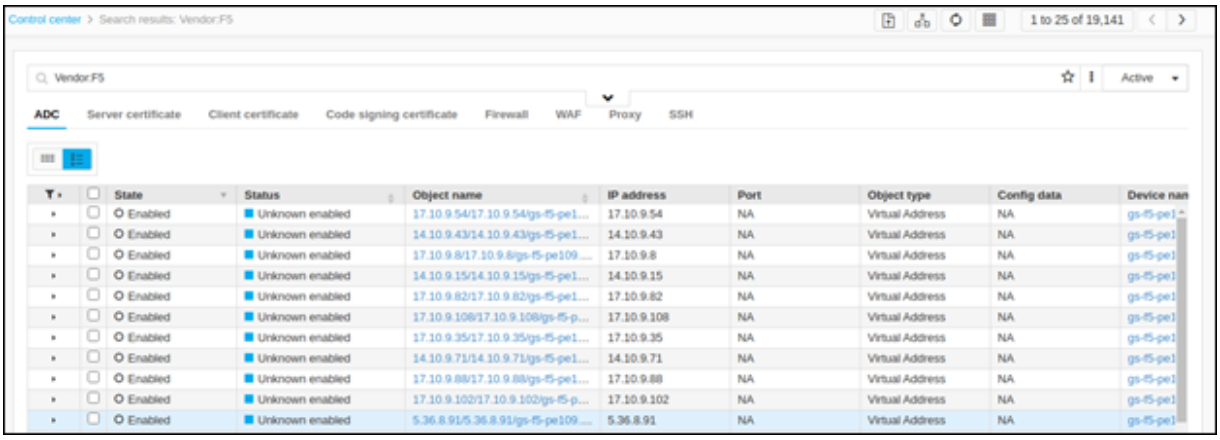


View the Object Details

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.

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:

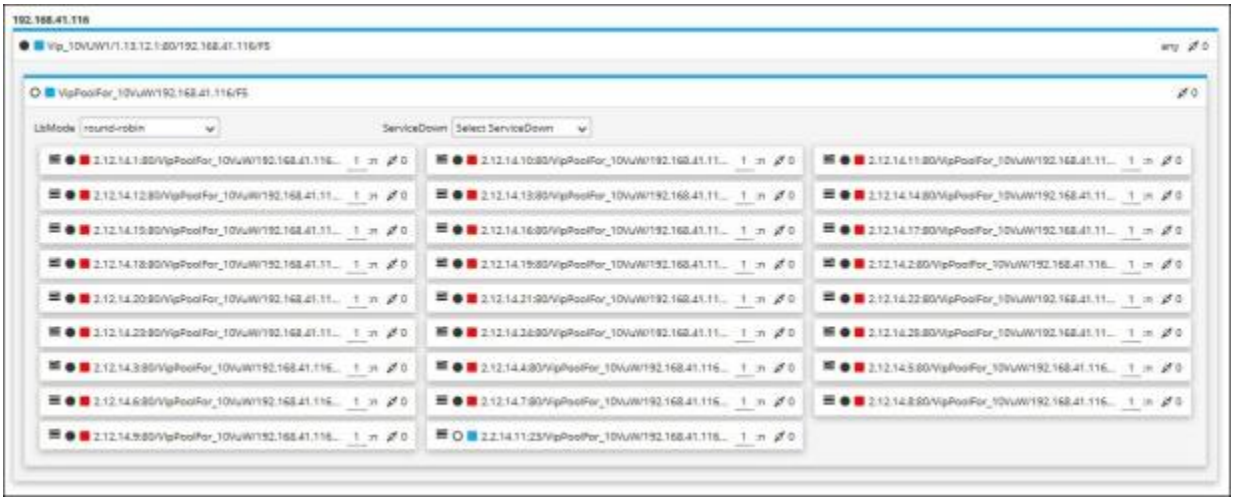
- **Topology View**: Clicking the object takes you to topological screens that provide much more information about the corresponding object than is displayed on the search results screen.
- **ADC Topology Actions**: ADC primary and secondary object search results can be right-clicked to view the list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

Topology View

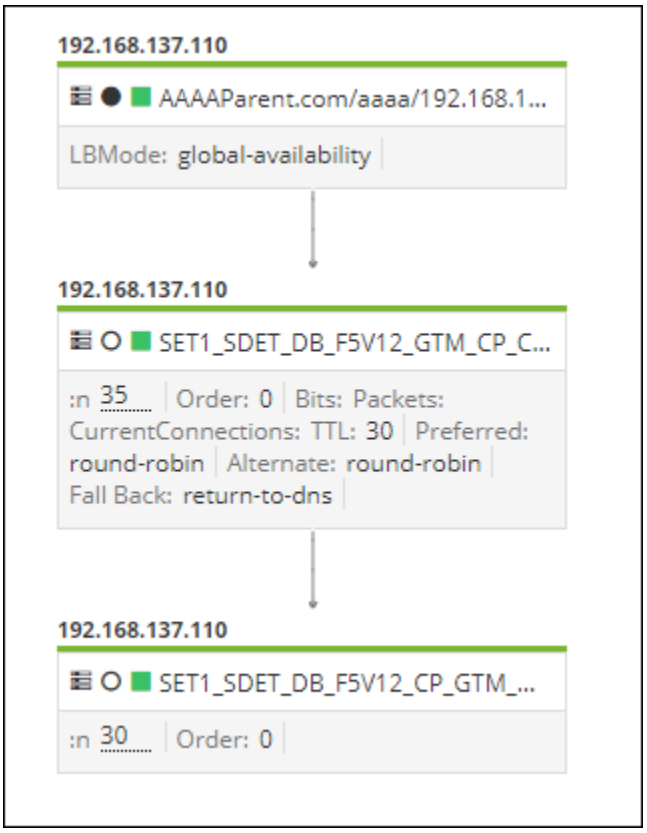
When you click a search result for a primary ADC object either from the **Application** or **Infrastructure** view, a topology view opens, providing a detailed, hierarchical map of the structure of the ADC. The following are the sample ADC topologies within the Control Center.

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

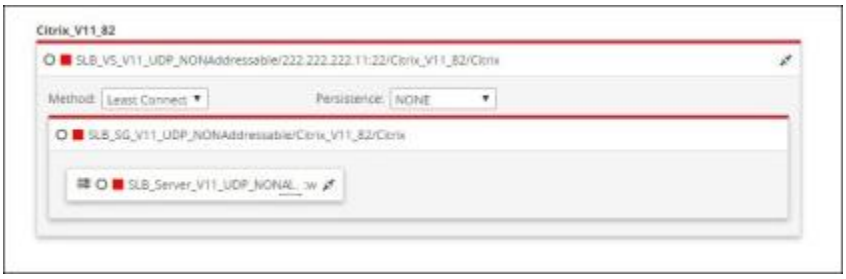
Virtual Server (VIP)/SLB Topology



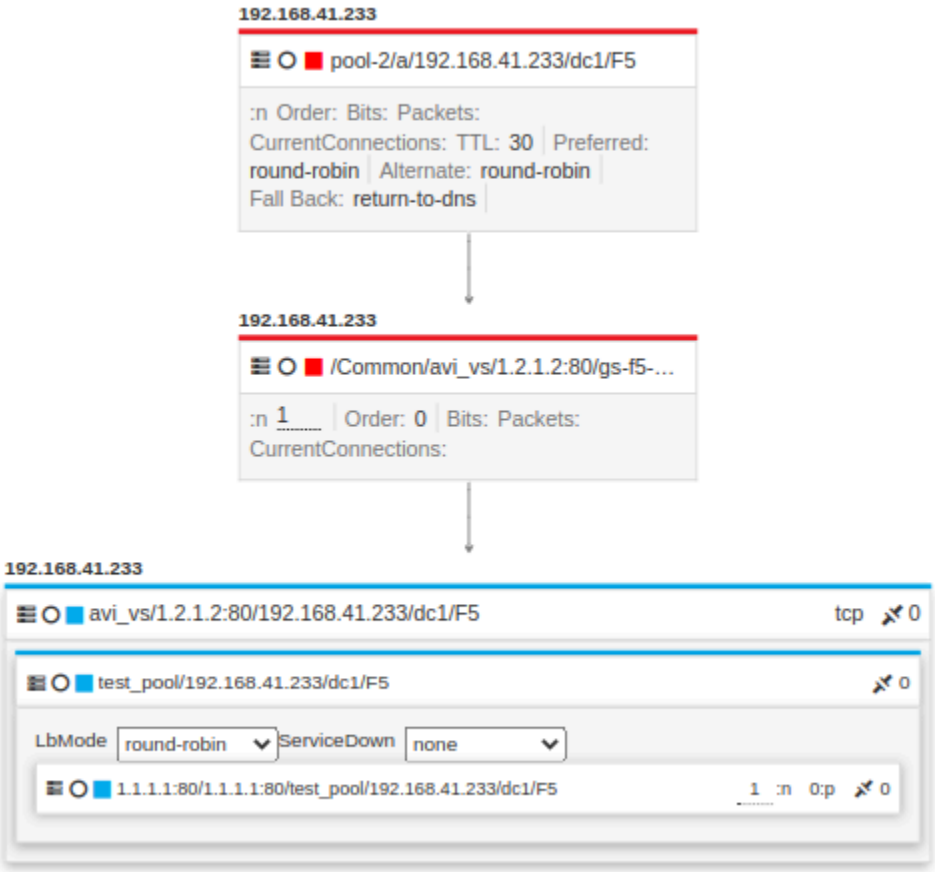
Wide IP/GSLB Topology



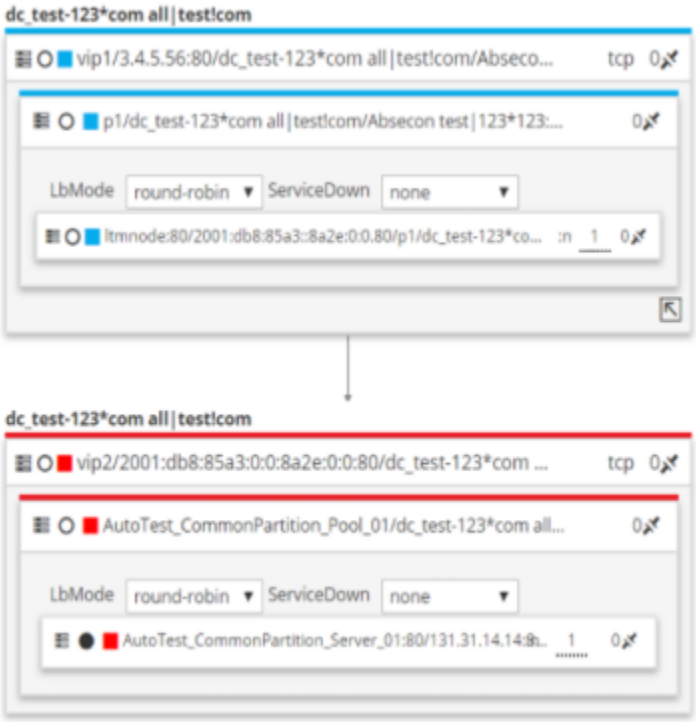
Server Load Balancing (SLB) Virtual Server Topology



Virtual Server (VIP) under Wide IP Topology



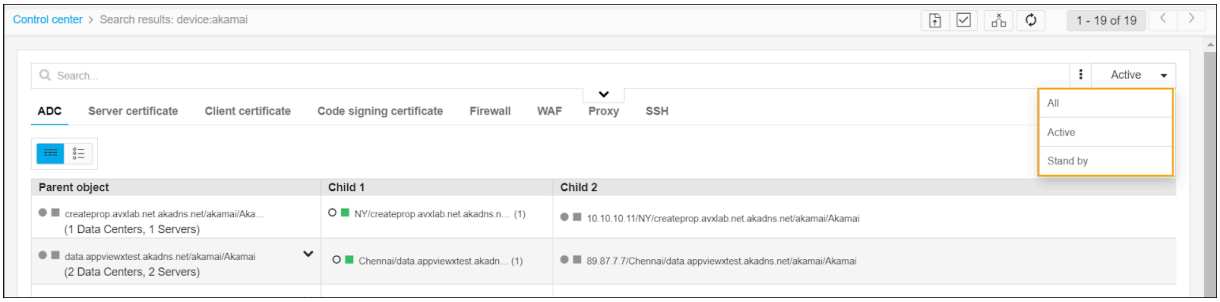
Virtual Server IP (VIP) under VIP Topology



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.

Access the Actions Menu for Objects on the ADC Search Results and Topology Screens

To access the actions menus for objects that appear on the ADC search results and Topology screens,

1. Click the **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **App Search**.
   The Control Center search screen appears.
2. Search for the ADC object whose actions menu you want to access.
3. In the search results field, you can do the following:
   - **Application View** - Right-click the object or one of its first or second-level children to view the list of actions you can perform.
   - You can multi-select or select all of the objects from the grid either by clicking the (**Select**) button beside the object or the (**Select all**) button in the Command bar.
   - **Infrastructure View** - Select the checkboxes beside the first column of the grid and then, click Actions to view the list of actions you can perform.
   - You can select all of the objects from the inventory by selecting the first checkbox in the grid.
   - Click the object's name in the search results field either from the Application view or Infrastructure view. The topology screen corresponding to the object you selected appears, right-click any of the components in the topology to view the list of actions you can perform.
     - The actions that appear in the list vary depending on the type of object you right-click as well as whether it is a parent or child, but the most common actions are listed below. To initiate any of the actions, scroll down in the list and click the corresponding action button.

Actions	Description
Enable	Enable an object.
Disable	Disable an object and terminate all active connections.
Graceful disable (AVI devices only)	Disable an object only when all the currently active client connections are closed by either the server or the client.

Actions	Description
Backup & Restore	• **Backup device** - Create a backup of the device associated with the object. For more details refer to the Create a Device Backup Group section of this guide. • **Restore object** - Restore object configuration to a previous state. For more details refer to the Restore an Object section of this guide. • **Compare** - To compare the objects with their associated devices. For more details, refer to the Compare ADC Objects section of this guide.
View	• **View graph** - View the timeline statistics of an object. For more details, refer to the View Timeline Statistics for an Object section of this guide. • **View config** - View the current configuration of all levels of the device object. For more details, refer to the View Configuration details section of this guide. • **View log/history** - View the log history of the object. • **View alerts** - View any alerts related to the object.
Compare config	Compare current and/or archived configurations of similar objects or the same object over time.
Clear persistence records (F5 devices only)	Clear the persistence records for VIP and pools.
View persistence records (F5 devices only)	View the persistence records for VIP and pools.
Advanced	• **Enable/Disable persistence** (F5 devices only) - Turn on or off 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. • **Enable/Disable all** (F5 devices only) - Turn on or off the object available across all the pools. • **Forcedown all** (F5 devices only) - Force shutdown of the object available across all the pools.

Actions	Description
View source connections (F5 devices only)	View the source connection IPs for VIP and pools.
Forcedown (F5 devices only)	Force shutdown of the object.
FD clear active connections (F5 devices only)	Clear active connections to the object.
Open in a new window	To display the topology view of the selected object in a new window.
Additional Actions on the Topology View	• **Ratio** - To modify the ratio of the pool member. • **Address Resolution Protocol (ARP)** - To enable/disable the ARP for the virtual address. • **Load Balancing (LB) mode** - To modify the load balancing method for the pools and service groups. • **Service down** - To control the connection management behavior of the pool. The following are the service-down settings that you can perform on the pool: Reselect, Reject, Drop, and None. • **Weight** - To modify the real server weight.

Compare ADC Objects

Comparisons are only possible for F5 ADC objects. Comparisons are also possible for multiple objects. You can select up to 5 devices to compare with the original device you selected.

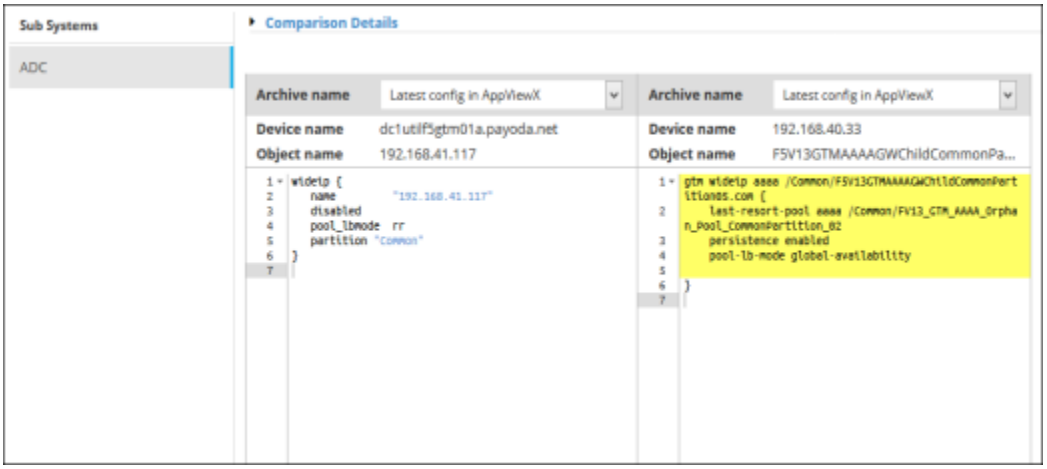
To compare ADC devices from the Control Center results within the App Search,

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

2. Run a search.

   By default, the search results are displayed in the  (**Application view**) page.

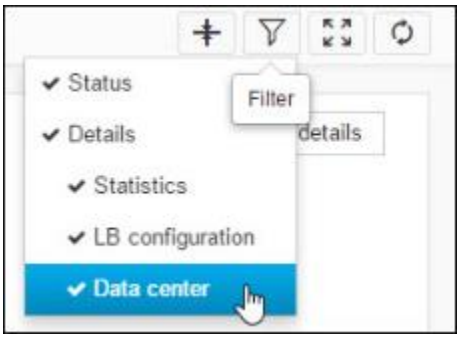
3. Click the  (**Select**) button beside each object in the list that you want to use in the comparison.
4. Right-click the selected objects and click **Compare config** from the dropdown list that appears.
5. If you want to compare configurations for the search results displayed on the infrastructure view, click the  (**Infrastructure view**) button to switch from the Application view search result page.
6. Select the checkboxes beside the first column of each object you want to use in the comparison and then, navigate to **Actions** > **Compare Config**.
7. The screen refreshes and displays the archived configurations side-by-side:



Filter the Information Displayed in an ADC Topology

To filter the information displayed in an ADC topology,

1. Open the ADC topology that you want to filter.
2. In the Command bar, click the  (**Filter**) button.
3. In the dropdown list that appears, deselect the type of information you want to filter out of the topology. Note that the abbreviation LB in the "LB configuration" filter refers to load balancing.



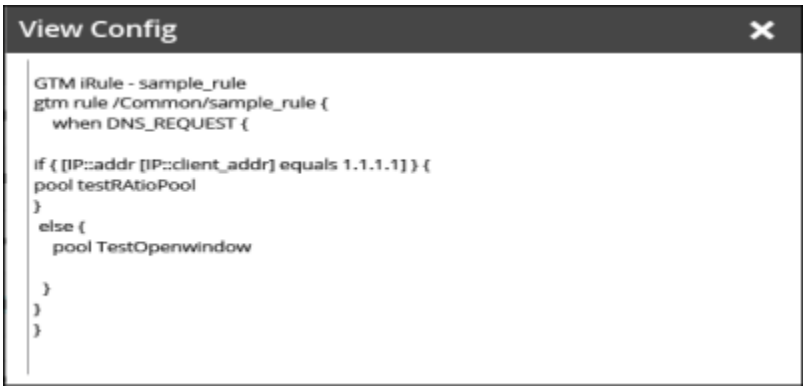
4. The topology updates and no longer displays the information you filtered out.

> **Note:** To turn off filters, repeat the steps above, but select, rather than deselect, the type of information you want to view.

View Configuration Details

To view the configuration details of the ADC device objects,

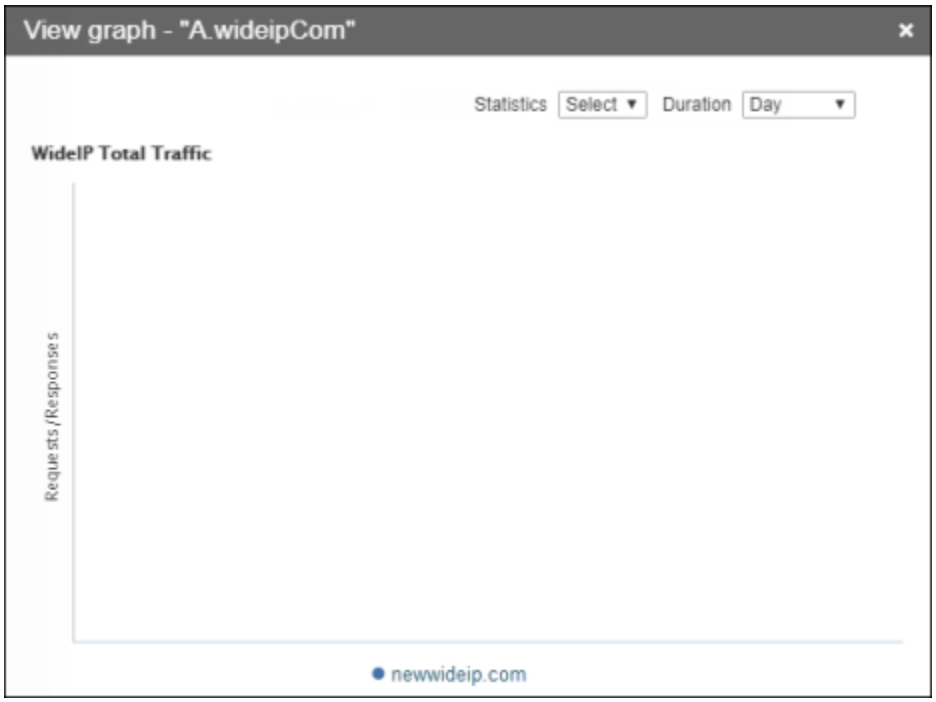
1. Click the **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **App Search**.
   The Control Center search screen appears.
2. Run a search.
   By default, the search results are displayed in the (**Application view**) page.
3. Right-click the device name and select **View** > **View config** from the dropdown list that appears.
4. If you want to view the statistics for the search results displayed on the infrastructure view, click the (**Infrastructure view**) button to switch from the Application view search result page.
5. Select the checkboxes beside the first column of each object details and then, navigate to **Actions** > **View** > **View config**. A popup screen appears, displaying the object's configuration as shown in the image below:



View Timeline Statistics for an Object

To view a customizable graph that displays timeline statistics for an F5, Citrix or A10 object visible through the App Search module,

1. Click the **Menu** > **ADC+** > **TRAFFIC MANAGEMENT** > **App Search**.
   The Control Center search screen appears.
2. Run a search.
3. By default, the search results are displayed in the (**Application view**) page. Right-click the device name and select **View** > **View graph** from the dropdown list that appears.
4. If you want to view the statistics for the search results displayed on the infrastructure view, click the (**Infrastructure view**) button to switch from the Application view search result page.
5. Select the checkboxes beside the first column of each object details and then, navigate to **Actions** > **View** > **View graph**. A statistics chart appears, displaying the following two fields at the top:
   - **Statistics** - The entries in this list vary depending on the device you selected. As you select different entries, the graph below updates to display the statistics related to the item you chose.
   - **Interval** - The following time intervals can be selected: **Day**, **Week**, **Month**, or **3 Months**. As you select different intervals, the graph below updates to display the statistics for the corresponding time frame.


View graph - "A.wideipCom"
Statistics
Select
Duration
Day
WideIP Total Traffic
Requests/Responses
newwideip.com

Chapter 3: ASSET MANAGEMENT

Asset Management Overview

AppViewX's ADC solution provides a single-pane-of-glass view of complex ADC infrastructure, supporting physical and virtual devices from the industry's leading ADC providers. It provides application-centric, customizable reports to help monitor application utilization and enable efficient capacity planning on the ADCs. It gives application and operation teams a topology view of the application delivery infrastructure for better visibility of their application. AppViewX can also project better insights into application health, state, status, utilization, and performance of applications from the managed network assets.

The ADC devices are managed/monitored under the following tabs within the Inventory:

- Device
- Groups
- Back-up & Restore

Supported ADC Vendors and Prerequisites

For supported ADC Vendors and prerequisites click here.

- Supported ADC Vendors and Prerequisites

Supported ADC Vendors and Prerequisites

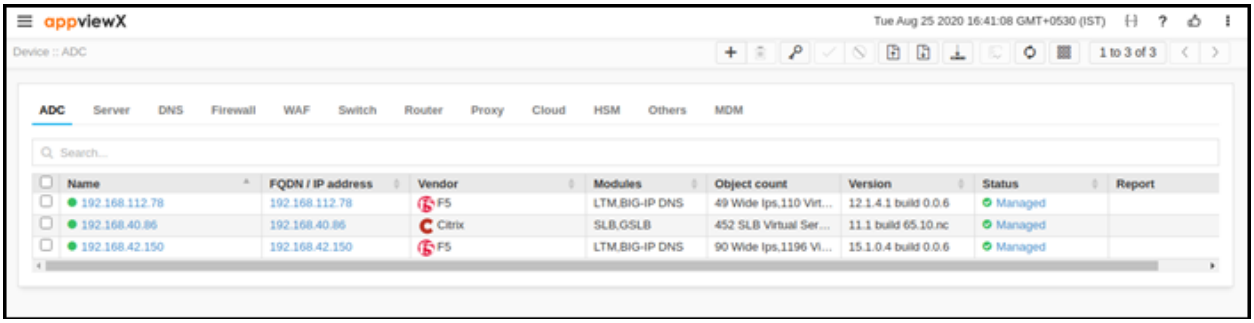
For supported ADC Vendors and prerequisites click here.

Device Inventory

- Manage and Unmanage Devices
- Export Device Details
- Manually Fetch the Configuration for a Device
- Generate and Download an iHealth Report
- Customizing Columns
- Configuration Sync between AppViewX and Device

Device Inventory Overview

Device inventory provides a birds-eye view of all the ADC devices onboarded into AppViewX. It is the single console where all the information about ADC devices such as number of objects, current status, Group Name, and version number will be displayed.



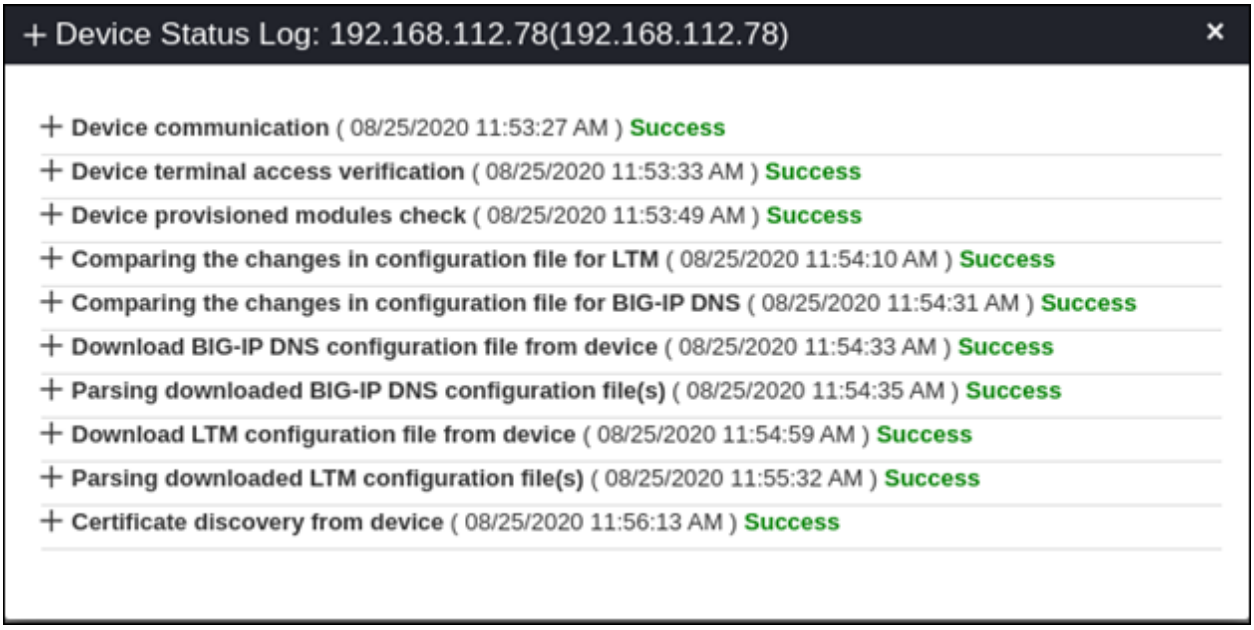
The ADC devices can be onboarded and managed from the Device Inventory. The complete details of the devices are available in the device Inventory for easy access and monitoring. Device Inventory gives you detailed information like name, IP, port, number of devices, current state and status, version, ADC provider, modules, and sync group name of the device.

Once the ADC device details are onboarded, devices must successfully go through the following setup process to be Managed into AppViewX,

- AppViewX tries to establish a connection with the device with the provided username and password. The communication protocol varies based on the ADC device providers.
- If the connection gets established, the required access is validated. For example, If any F5 ADC device gets added, Terminal access verification happens from AppViewX.
- The requested module is validated in the ADC Device. For example, if an ADC device is added as GSLB, then the appropriate provision is validated.
- The version of ADC device is fetched and validated for the supported version.

- The configuration is fetched from the device through REST or any other supported protocol by the ADC device provider. The configurations are made available in AppViewX.
- If the certificate discovery is enabled, then appropriate certificates from the ADC device are discovered.
- If secondary device detection is enabled, then failover/standby device information is fetched.

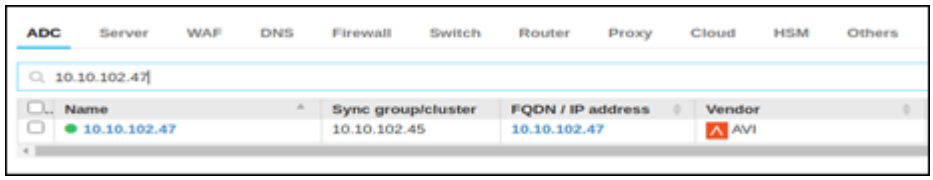
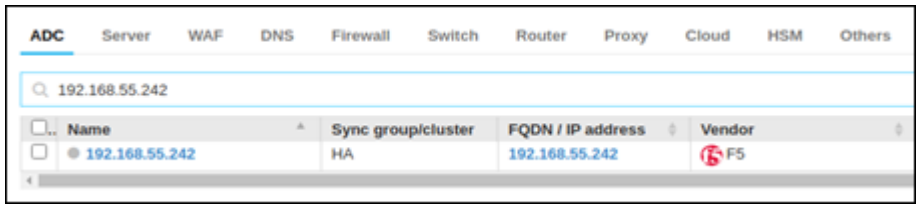
The progress of these steps can be viewed in the inventory by clicking the status column of the device. By clicking the (+) button, detailed information will be available for each step.



- Device State
- Device Status

Device State

High Availability of the applications can be ensured by configuring ADC devices in Active-Standby mode. This type of configuration will be planned for disaster recovery. In some cases, the devices in the group will be in active-active mode for handling the traffic efficiently. In AppViewX, the current mode of the device is called state and it will be displayed along with the device name in the inventory page. The device will be in any one of the following states,

State	Color Code	Description
Active	Green Circle	The device is currently processing the traffic of the application in the Active-Standby setup. 
StandBy	Orange Circle	The device will be ideal and ready to take over whenever the failover occurs in the Setup. 
Offline	Grey Circle	The device is taken down for maintenance and in this state, the traffic will not be passed through the device. 

Toknow the current state, mouse over the color icon available before the device name.

This state will get updated in a particular time interval during configuration fetch from the device.

For F5 and Citrix, if Syslog is enabled, it will get a near real-time update whenever there is a flip in the device.

Device Status

On adding the ADC device into AppViewX, the status defines the current stage of device configuration parsing in AppViewX. This data will be available as a separate column in the device inventory page. The device will be in any of the following statuses in the inventory and the detailed progress can be viewed by clicking the status image,

Status	Symbol	Description
Queued	Queued	The device details are added in AppViewX and waiting for configuration fetch to start from the ADC device.
Inprogress	Inprogress	It states that the communication to the device is successful and configuration fetch from the device is yet to be completed.
Managed	Managed	All the configurations from the added device are pulled, parsed, and available in AppViewX. This stage states that the device is successfully onboarded into AppViewX.
Unresolved	Unresolved	AppViewX could not connect to the device due to communication or credentials issues.
Failed	Failed	AppViewX established a connection with the device but the device configuration parsing was failed due to some exceptions. The detailed reason for failure can be known by clicking the Failed icon itself.
Unmanaged	UnManaged	If any maintenance activity needs to perform on a device, then the device can be moved to this stage in AppViewX by clicking the () button on the top right corner of the inventory page. In this stage, AppViewX will not trigger any communication to the device. Whenever required, the device can be managed again by clicking ().

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.

Search for ADC Devices

Devices that are added to AppViewX can be found in the inventory by searching it by name in the search bar.

To search for objects,

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Enter the search keyword in the **Search** field.
   The devices that match the search keyword are displayed.
3. The search term can be any of the device details like name, IP, provider, version, status of the device, sync group name, etc.
4. You can also search based on sync group or custom group name to see the devices available in a particular group.

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.

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.

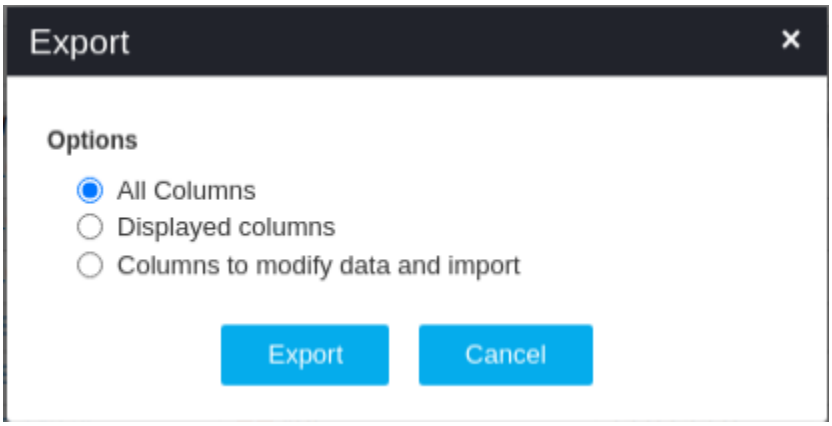
3. Click the checkbox beside the device name.
4. To start managing the device, click the **Manage** button in the Command bar at the top of the screen. To stop managing a device, click the **Unmanage** button.

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.

Manually Fetch the Configuration for a Device

If the latest configuration in the device needs to be pulled into AppViewX, those devices can be selected and fetch config can be triggered. AppViewX will communicate with the device and pull the latest configuration available in the device and persist in AppViewX.

To manually get the configuration for a device,

1. Go to ☰ **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. If the device is not listed on the screen, run a search to locate it.
3. Click the checkbox beside the device name. If you want to fetch configurations for multiple devices of the same type, select their checkboxes, too.
4. Click the  **Fetch Config** button in the Command bar.
5. A notification appears at the top of the screen stating, "**Fetch config has been triggered for the device(s).**".

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.

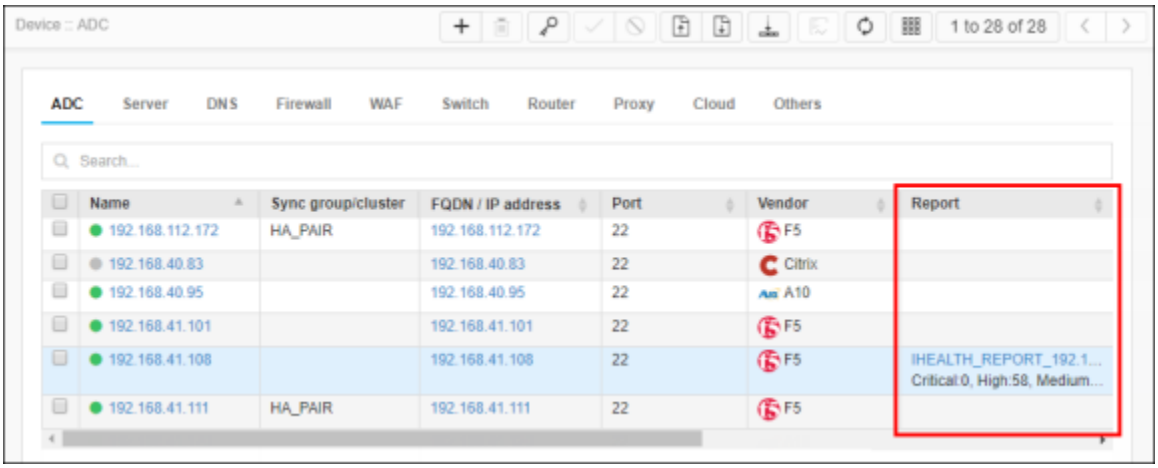
- iHealth reports can be generated at the time you want to view or schedule it in advance through the Workflow.
- To generate an iHealth report, ensure that the proxy is configured in the Settings module. For detailed information, refer to the Proxy Settings section of Platform User guide.

To generate and download an iHealth report,

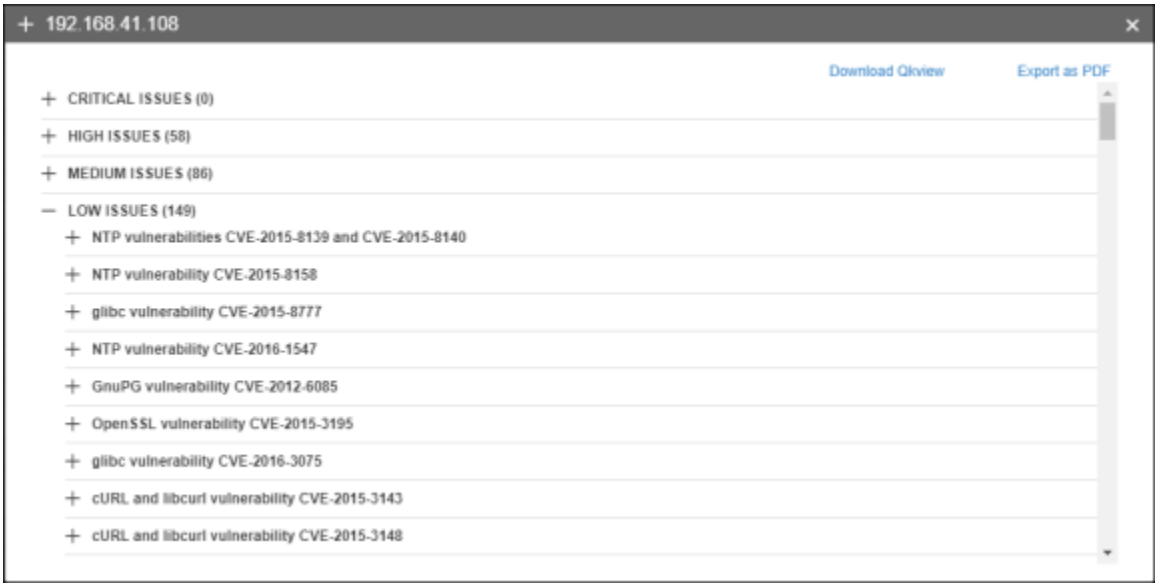
1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**
   By default, the **ADC** tab opens.
2. Select the checkbox beside the ADC device for which you want to generate an iHealth report.
3. Click the **Generate iHealth Report** button in the Command bar.

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

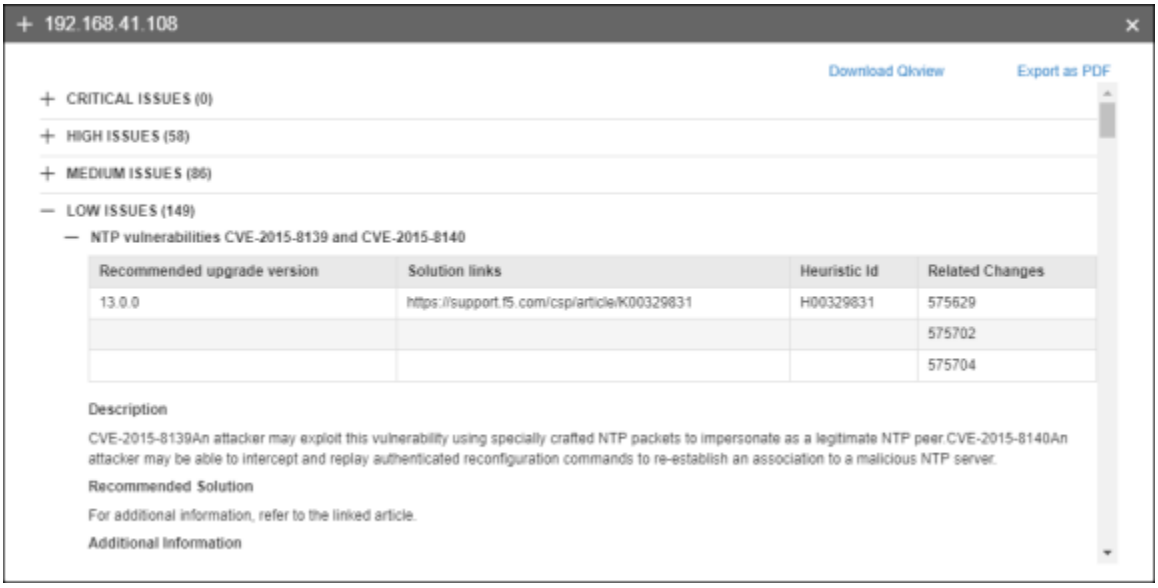
4. On the iHealth Report Generate screen that pops up, enter the case number for the report, then click Generate.
5. When the report is generated, it appears as a link in the Report column on the Device: ADC screen.
6. Click the IHEALTH_REPORT link.



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.



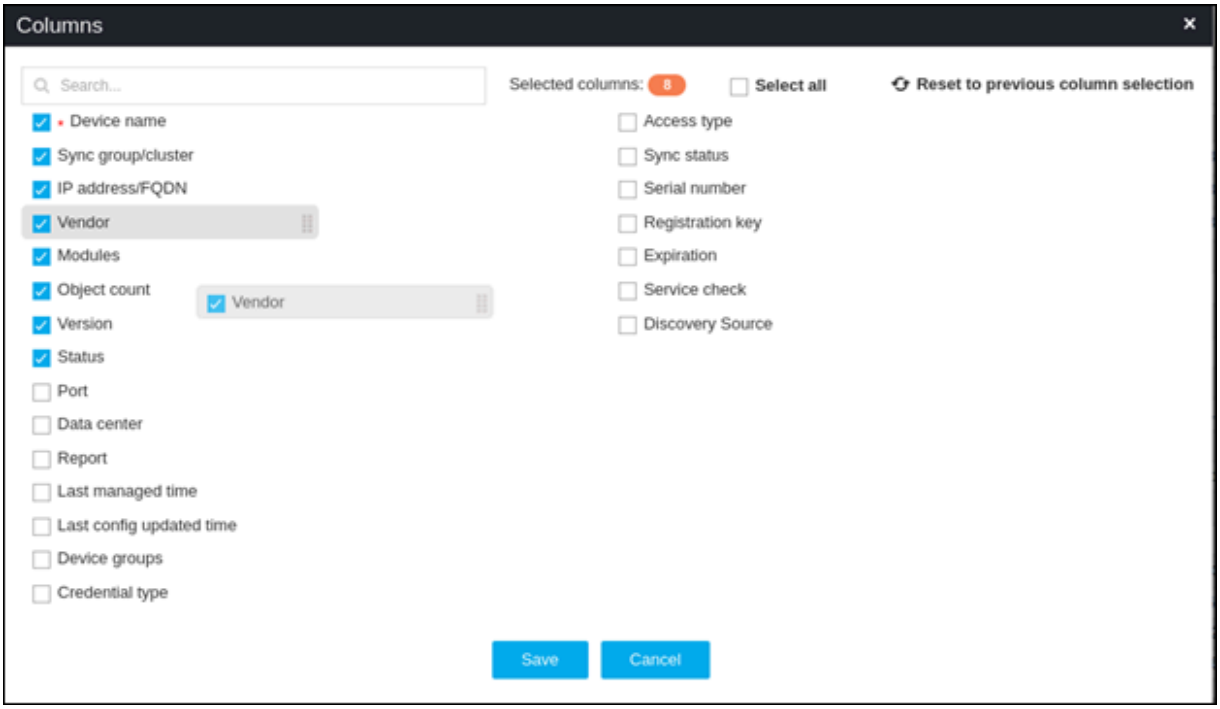
10. (Optional) Download the entire iHealth report as a Qkview file by clicking the **Download Qkview** link or as a PDF file by clicking the **Export as PDF** link, both of which appear in the top right corner of the screen.

Customizing Columns

The columns in the Device Inventory page are highly customizable as per the user's convenience. Any column can be hidden, added, or alter the order of the columns.

To customize columns,

1. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**.
   By default, the **ADC** tab opens.
2. Click the **Columns** button in the Command bar.
   The **Columns** pop-up opens.



3. In the Columns pop-up, you can modify the columns by doing any of the following or in the combination:
   a. Select or deselect the desired columns to be displayed in the **ADC** tab.
   b. Alter the order of the column by dragging the column name to the desired order.
   c. Select all the available columns by clicking the **Select all** checkbox.
   d. Reset to the previous column selection by clicking the "**Reset to previous column selection**".

4. Click the **Save** button.

> **Note:** To discard the changes, click the **Cancel** button.

Configuration Sync between AppViewX and Device

The device configuration will be fetched into AppViewX periodically. By default, this process happens automatically at 12:00 AM everyday. The time and days can be configured as per the custom demand. For more detail, see Settings.

Onboard Device

- Discover/Onboard an ADC Device
- Vendor Specific DiscoverOnboard 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.

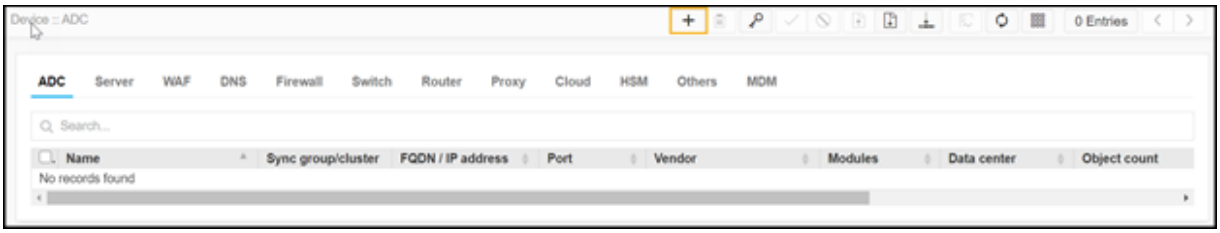
After navigating to **Menu** > **ADC+** > **ASSET MANAGEMENT** > **Device Inventory**, you can also add devices under the DNS, WAF, or Others tab. Under the following tabs, you can

- **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 use them in ADC automation workflow.
- **WAF** - add a device to identify the vulnerability using ADC automation workflow.

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

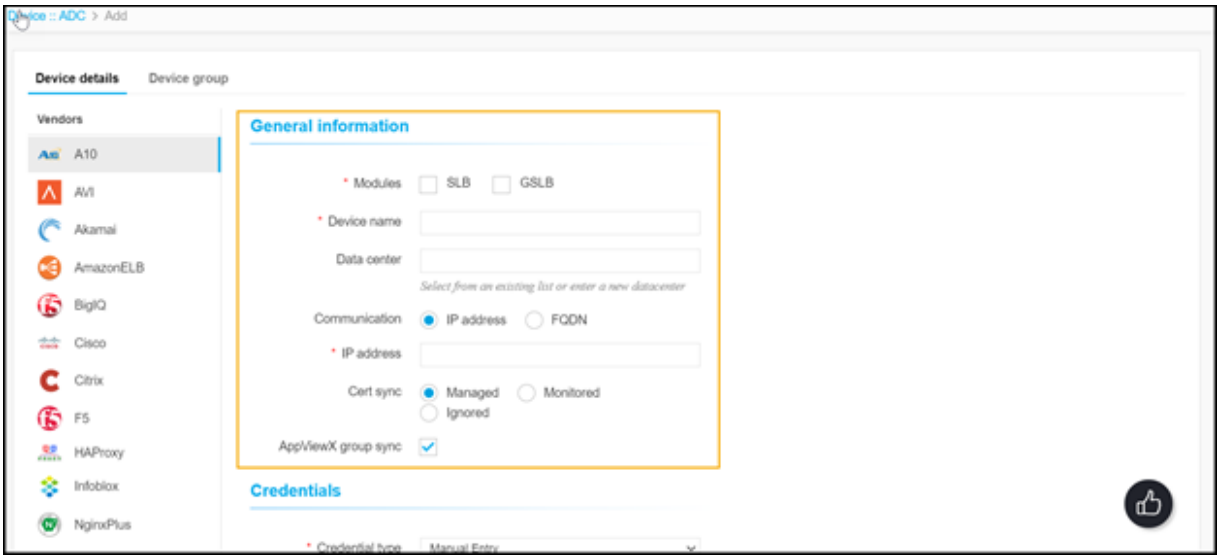
To onboard a device into Device Inventory,

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.



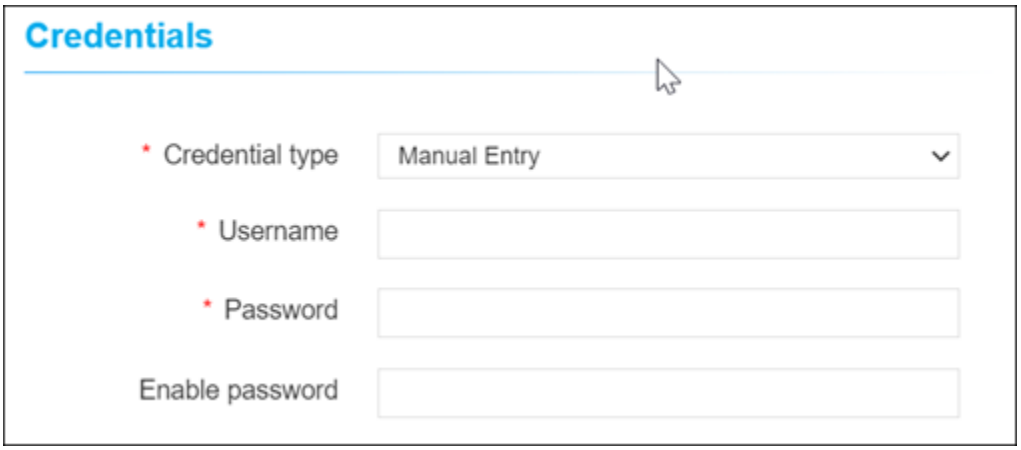
The following table provides the field description for adding ADC device details in the **General Information** page:

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.

Field	Description
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 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 SETTINGS page.

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

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

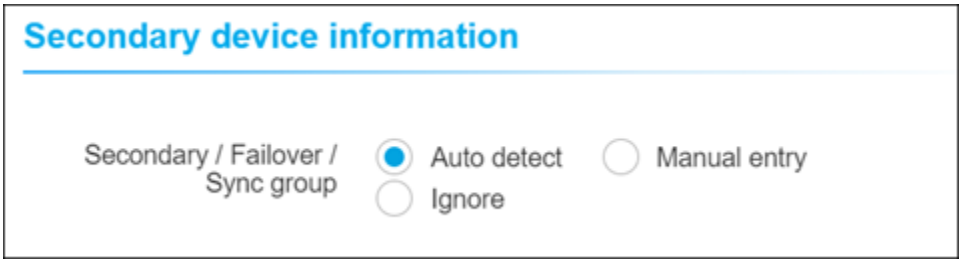


The following table provides the field description for adding ADC device details in the **Credentials** page:

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. 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).

Vendor Specific DiscoverOnboard ADC Device

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

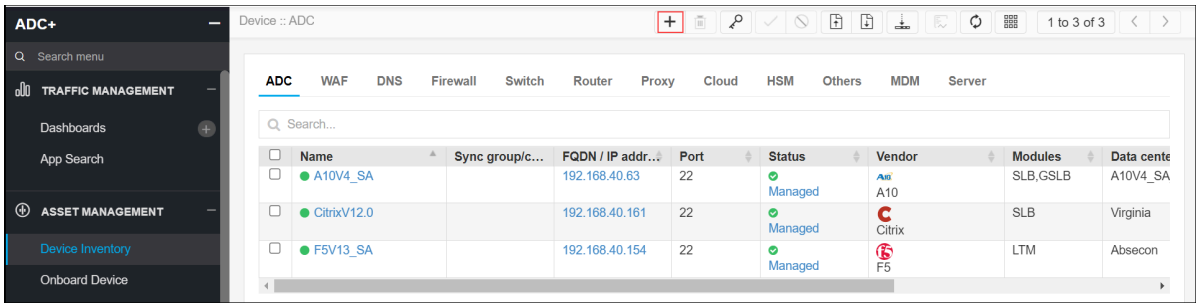
A10

- Adding A10 Device
- Validating the A10 device addition

Adding A10 Device

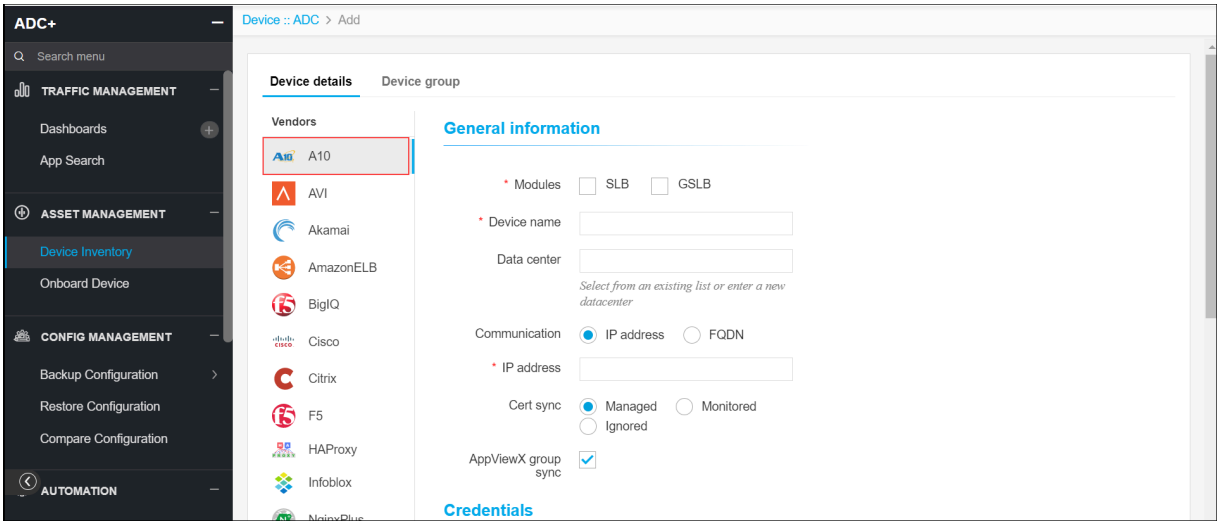
To add A10 device,

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.

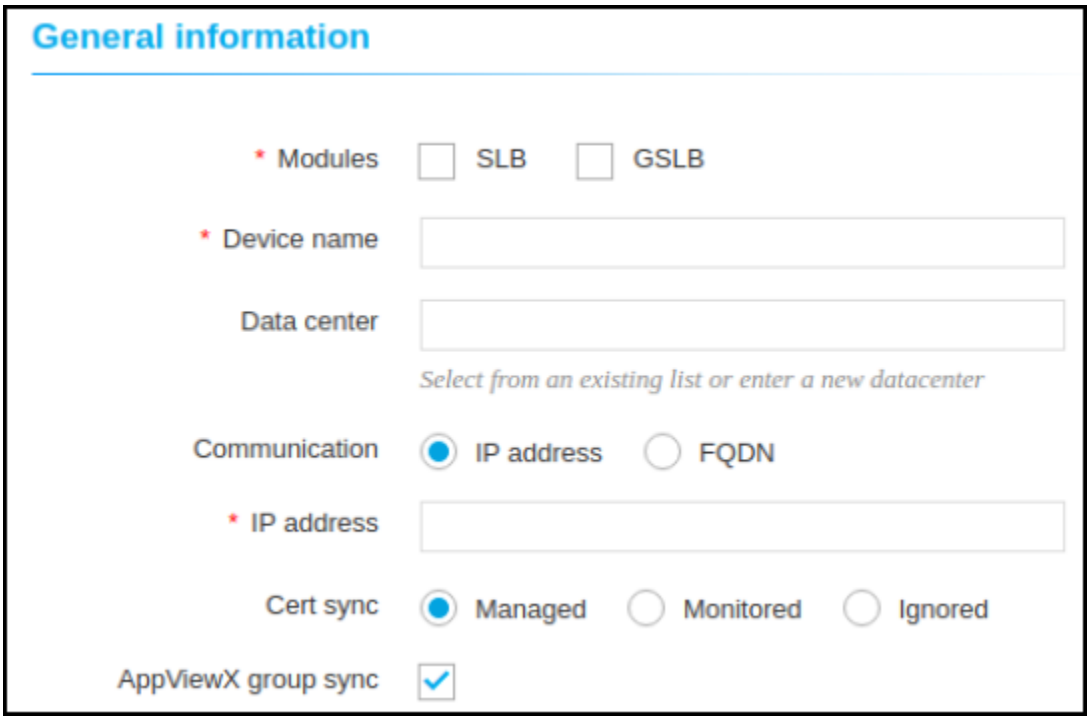


- Click **Onboard Device** in the left navigation panel.

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



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

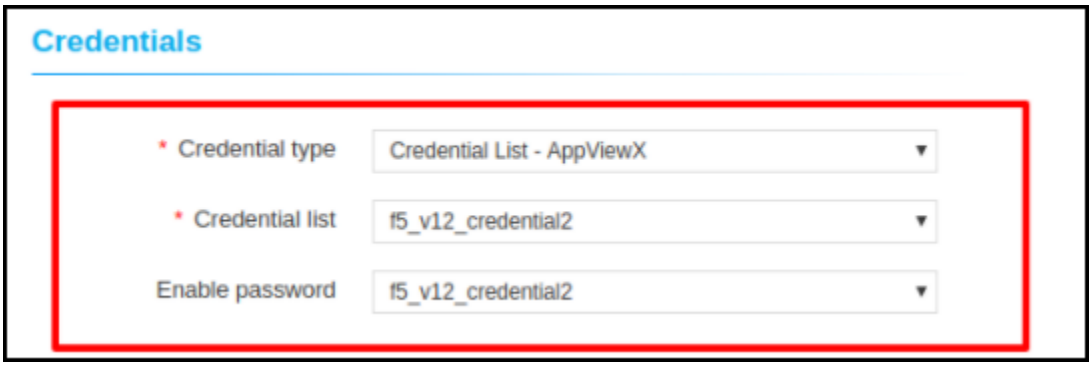


6. The following table provides the field description for adding ADC device details in the **General information** section:

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.

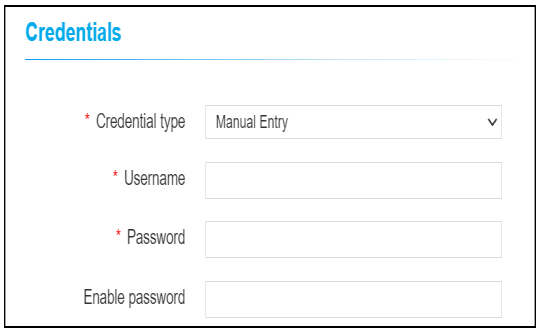
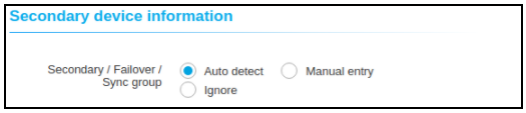
Name	Type	Mandatory	Description	Validation
FQDN	Text	Yes	The FQDN of the device.	the FQDN should be in a valid format.
Cert Sync	Radio button	Yes	Managed: The certificates of the device can be managed. Monitored: The certificates of the device can be monitored. Ignored: The certificate sync can be ignored.	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**.

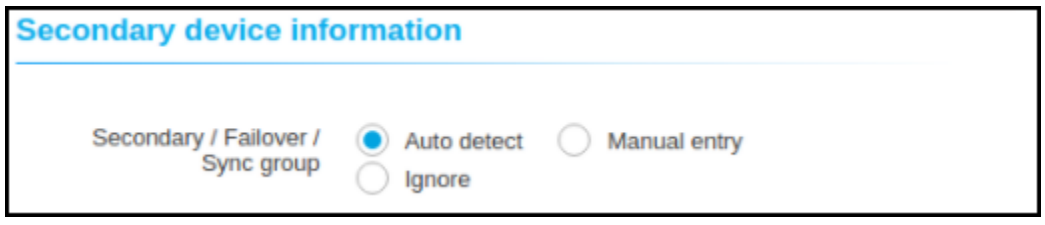


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
Credential type	Dropdown	Yes	Manual entry:	NA

Name	Type	Mandatory	Description	Validation
			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.  	
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.



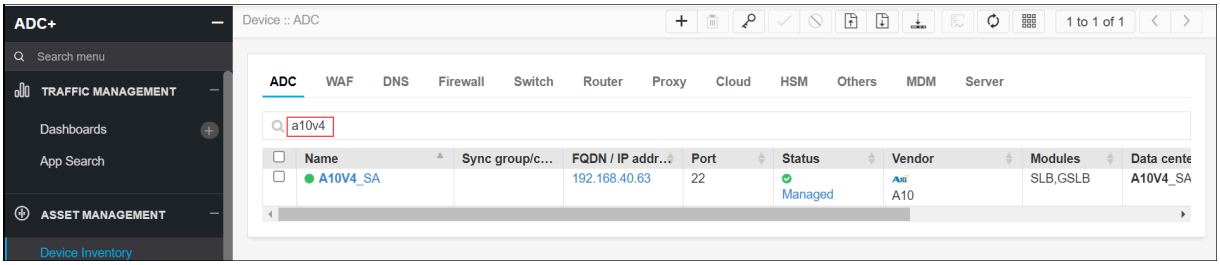
10. The following table provides the field description for adding ADC device details in the **Secondary device information** section:

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.

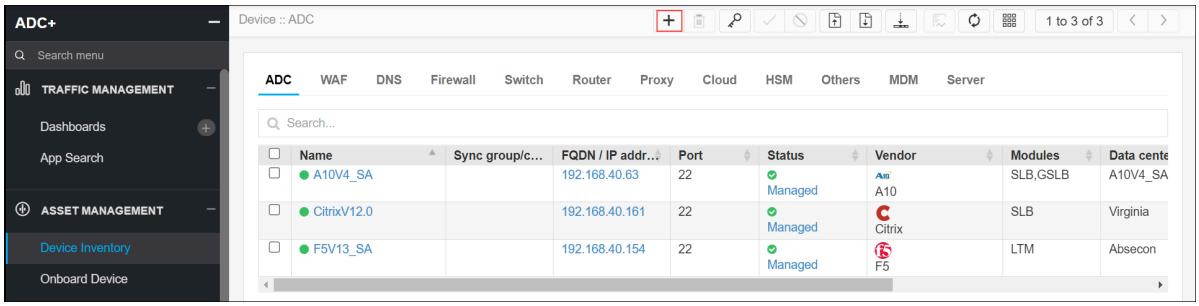


AVI

Adding AVI Device

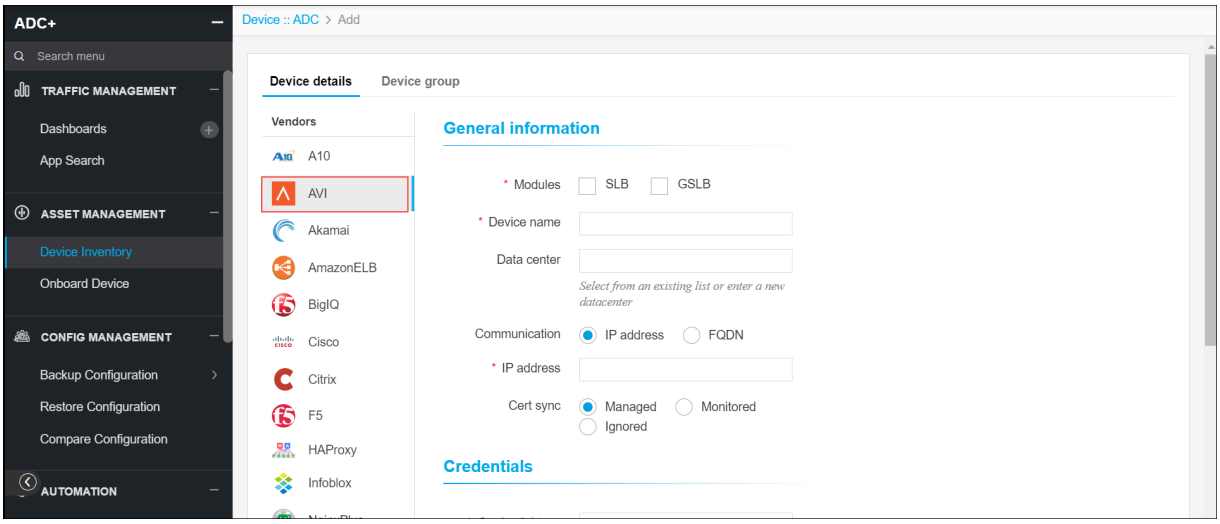
To add AVI device,

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.

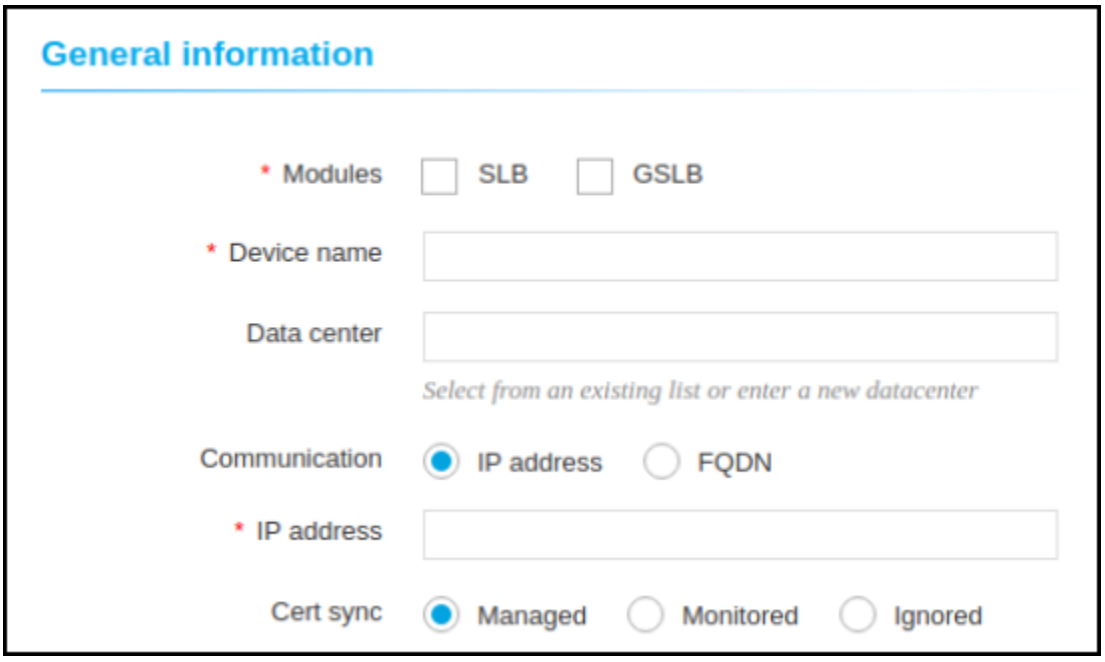


   - Click **Onboard Device** in the left navigation panel.

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



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

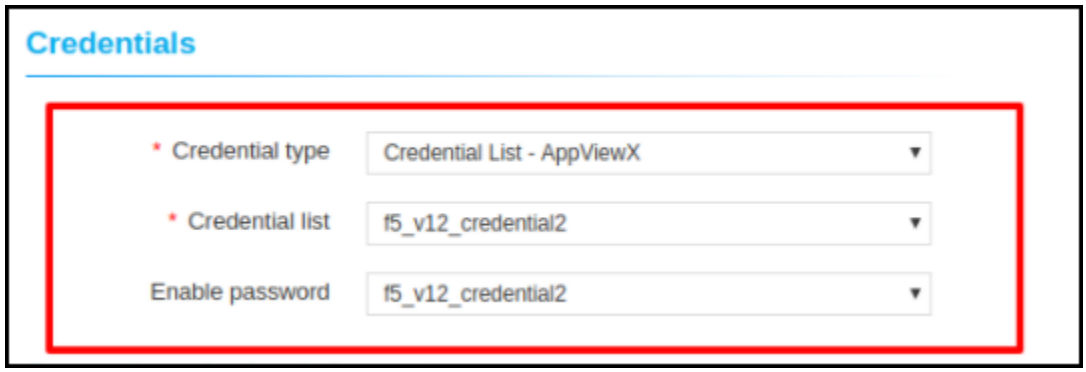


6. The following table provides the field description for adding ADC device details in the **General information** section:

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

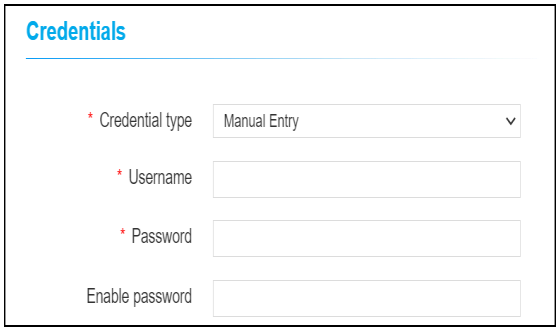
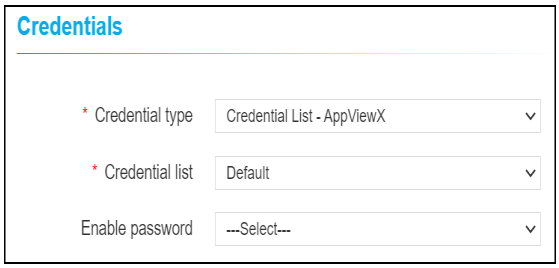
Name	Type	Mandatory	Description	Validation
Cert Sync	Radio button	Yes	**Managed**: The certificates of the device can be managed. **Monitored**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA

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

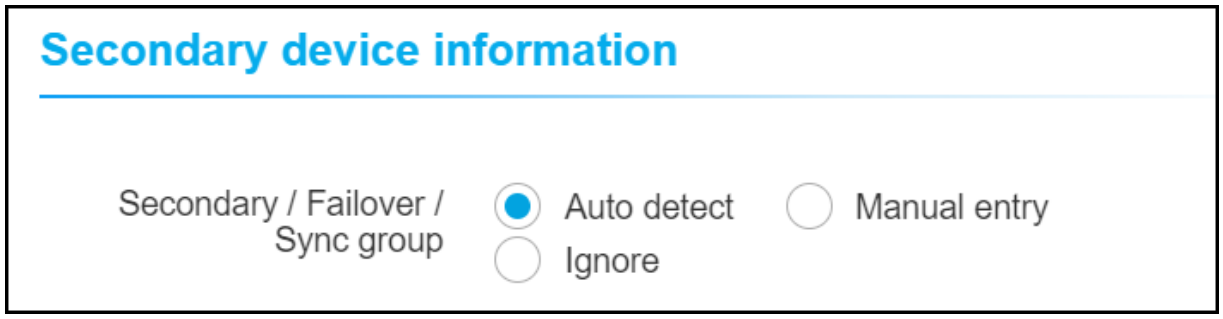


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

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

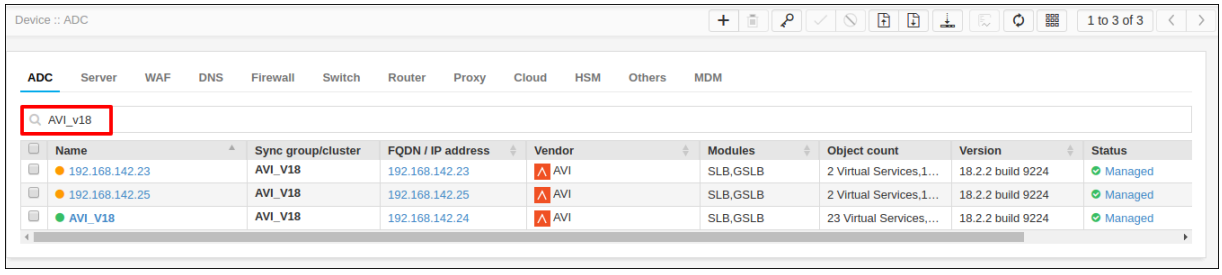
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The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

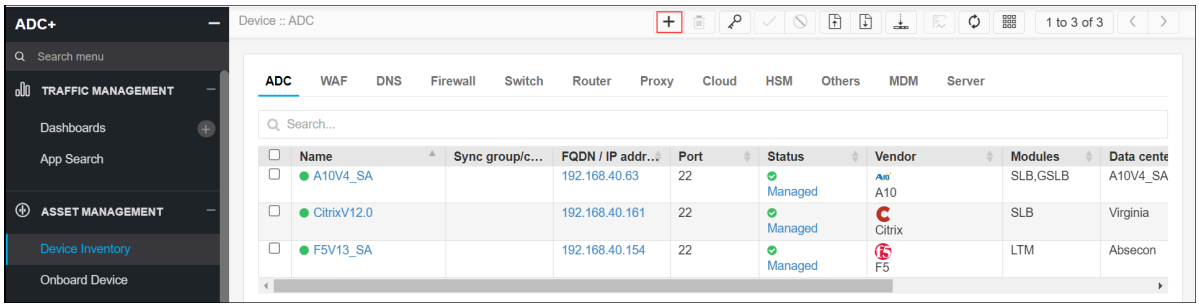


Akamai

Adding Akamai Device

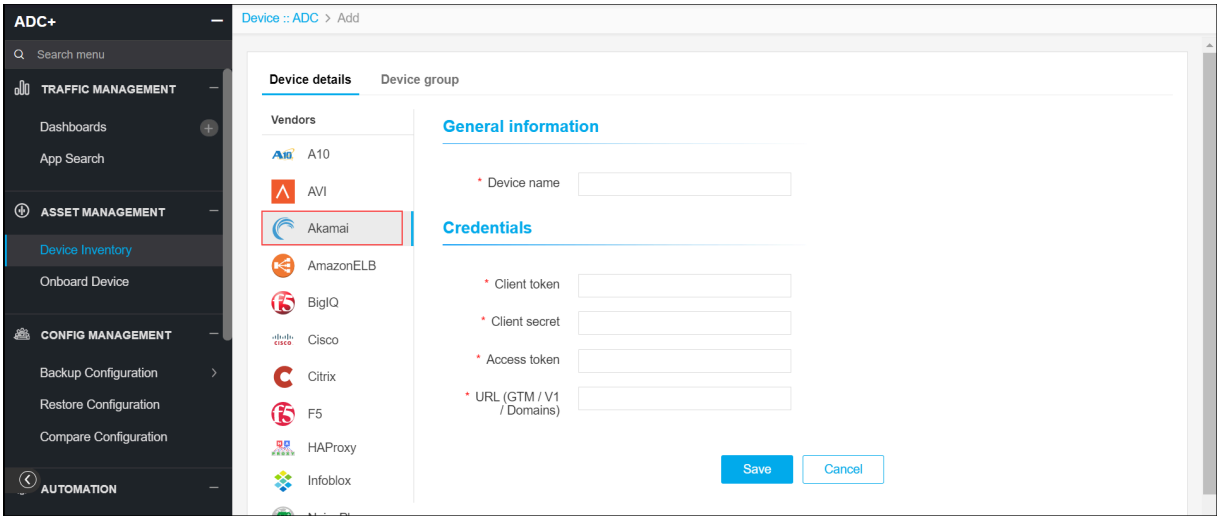
To add Akamai device,

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.

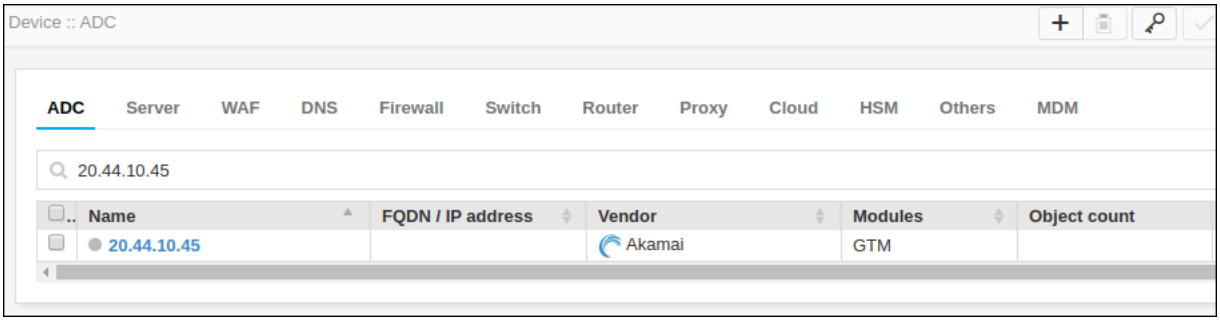
Name	Type	Mandatory	Description	Validation
*Device name	Text	Yes	Unique name of the device to be added.	Device name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
*Client token	Text	Yes	Client token of the Akamai device.	NA
*Client secret	Text	Yes	Client secret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

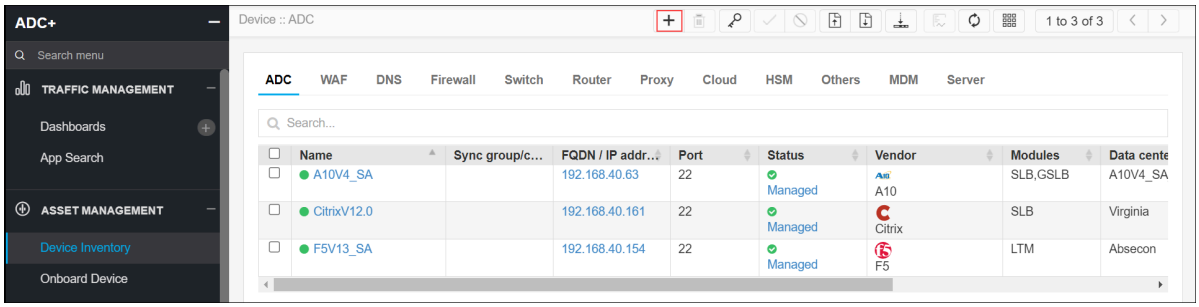


Amazon ELB

Adding Amazon ELB

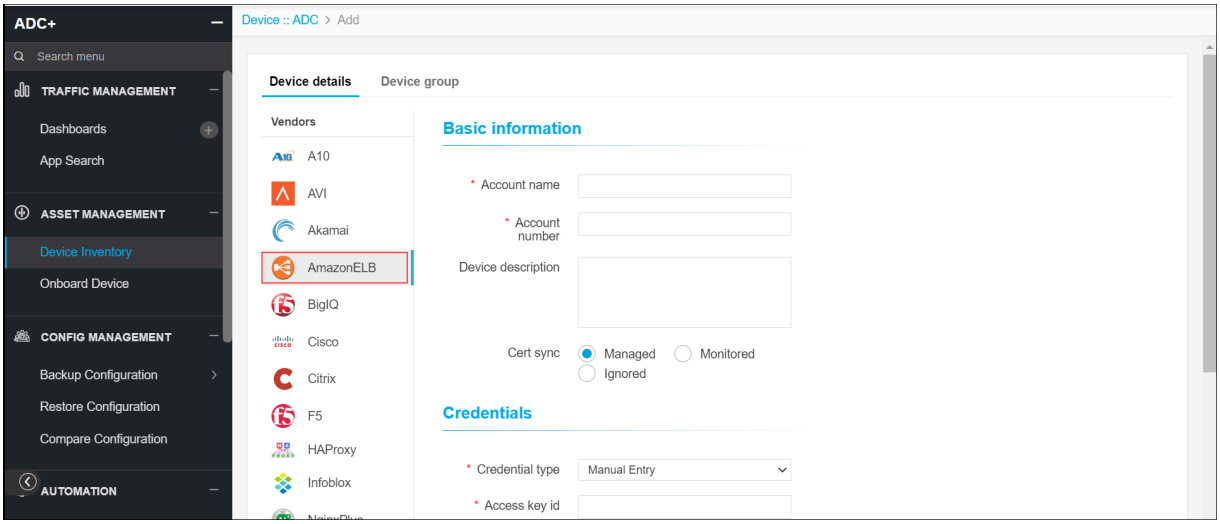
To add Amazon ELB,

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.

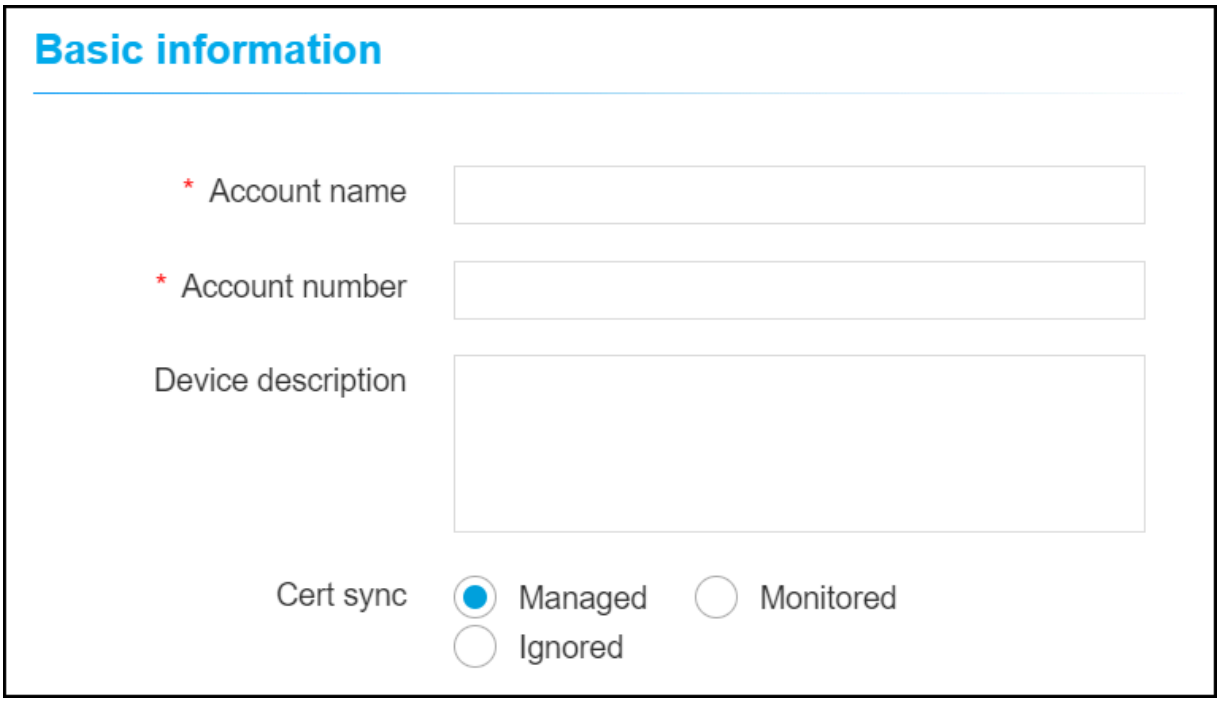


   - Click **Onboard Device** in the left navigation panel.

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



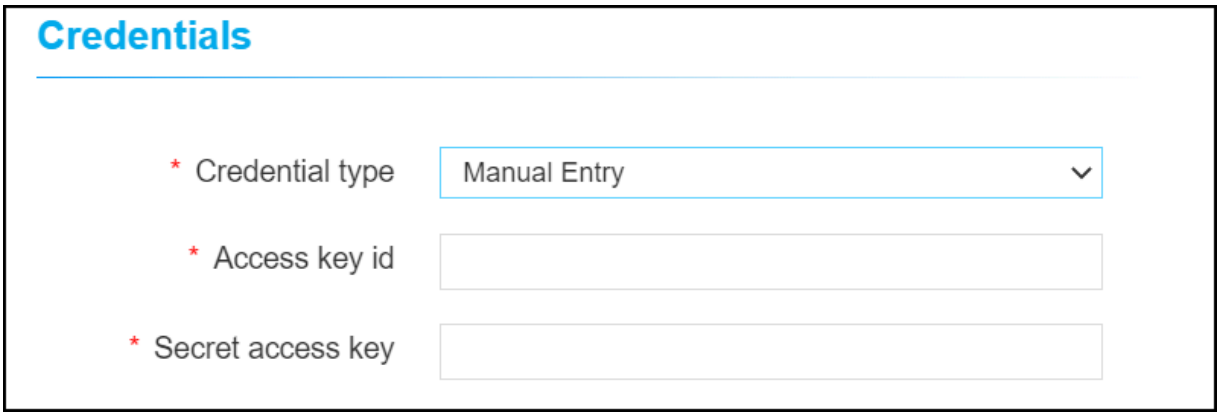
5. Enter or select the field information in the **Basic information** section.



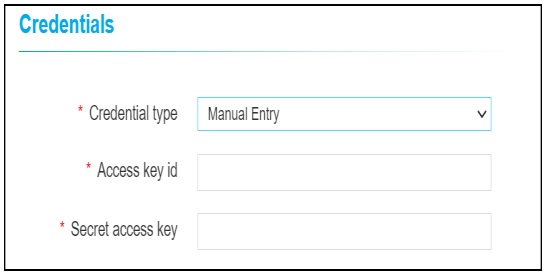
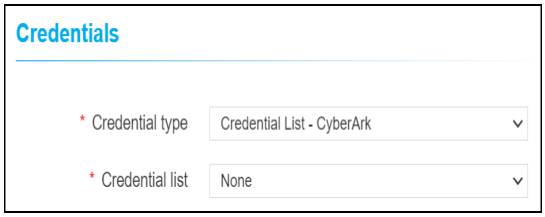
6. The following table provides the field description for adding ADC device details in the **Basic information** section:

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

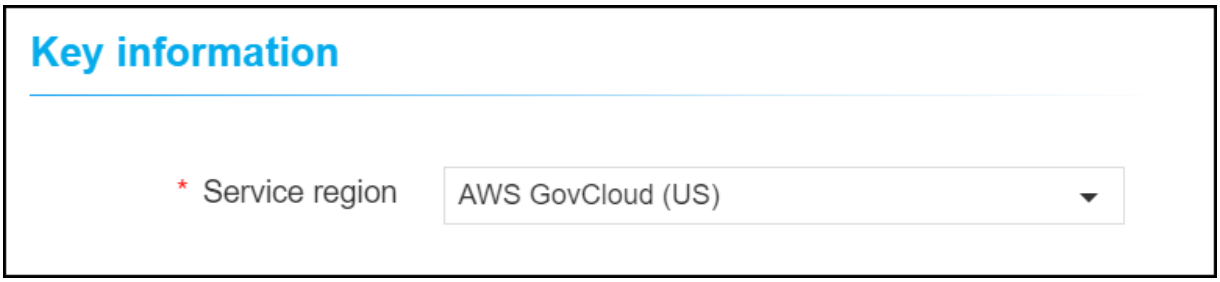


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

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

Name	Type	Mandatory	Description	Validation
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:

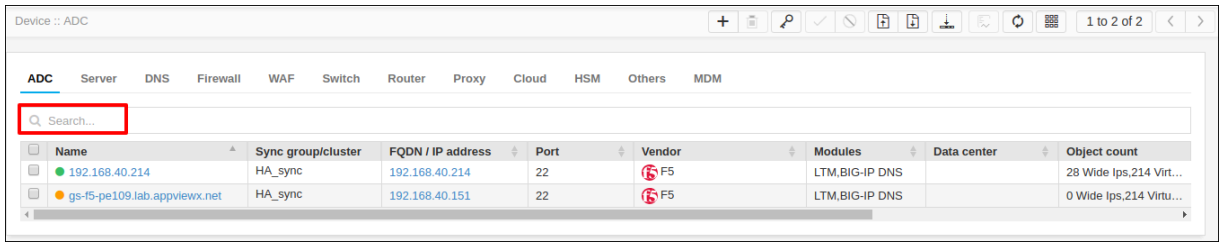
Name	Type	Mandatory	Description	Validation
Service region *	Dropdown	Yes	Service region of the AmazonELB device.	NA

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.

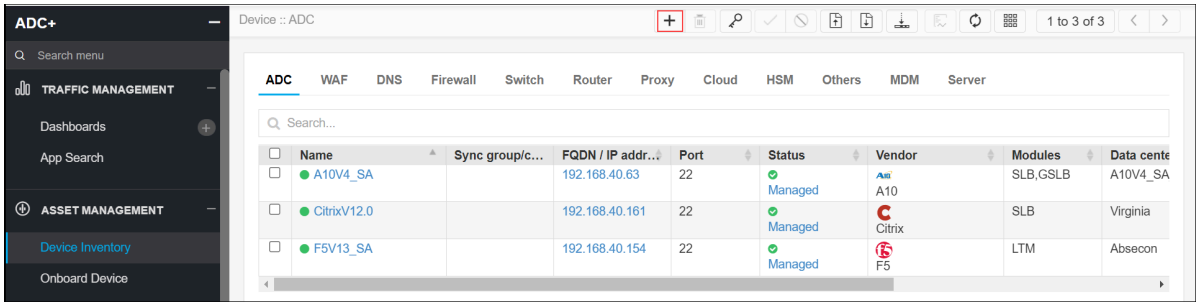


BigIQ

Adding BigIQ Device

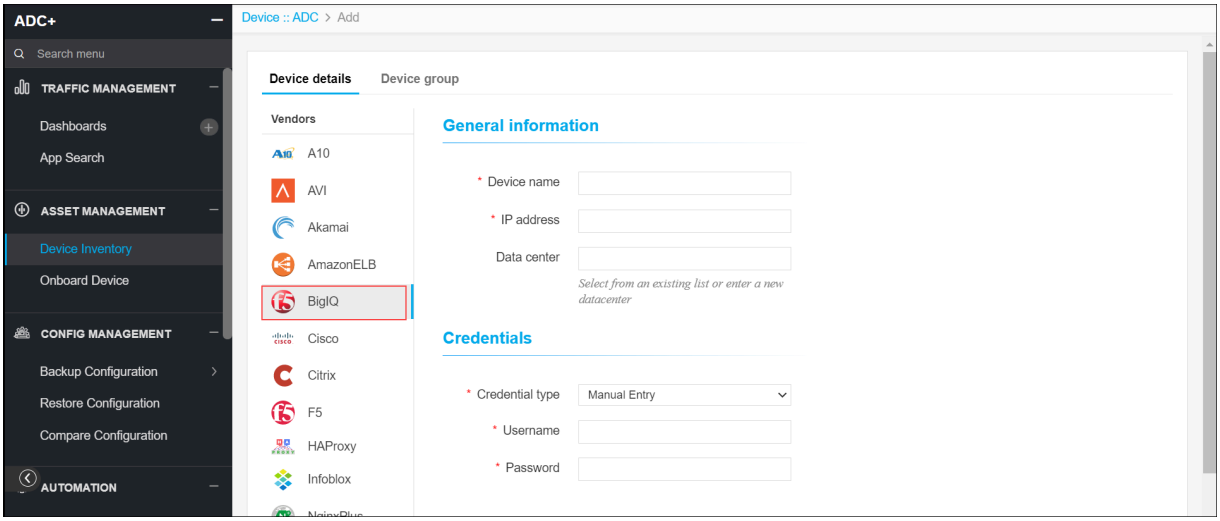
To add BigIQ device,

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.

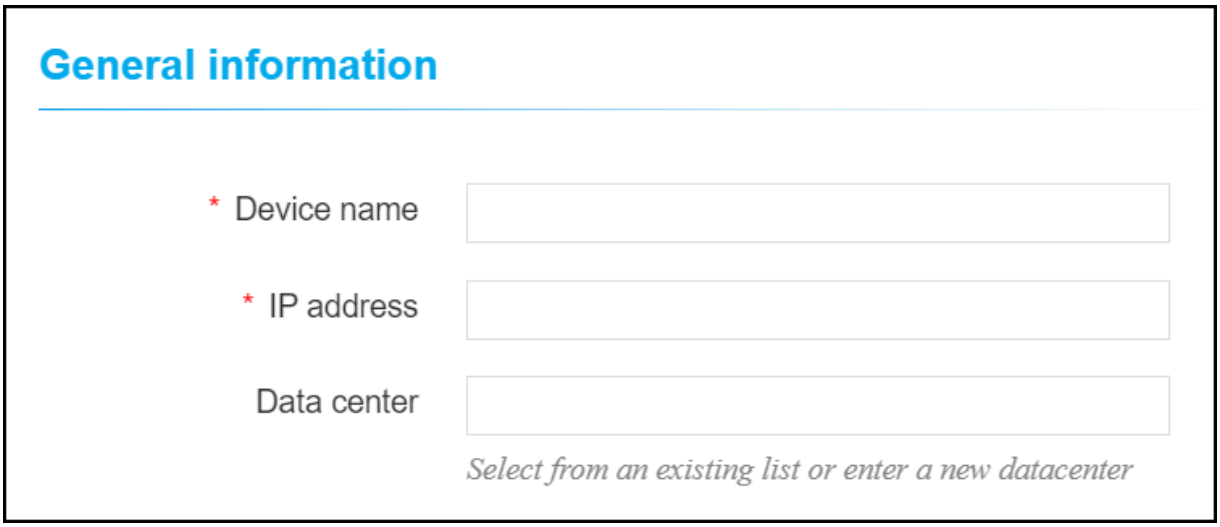


   - Click **Onboard Device** in the left navigation panel.

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



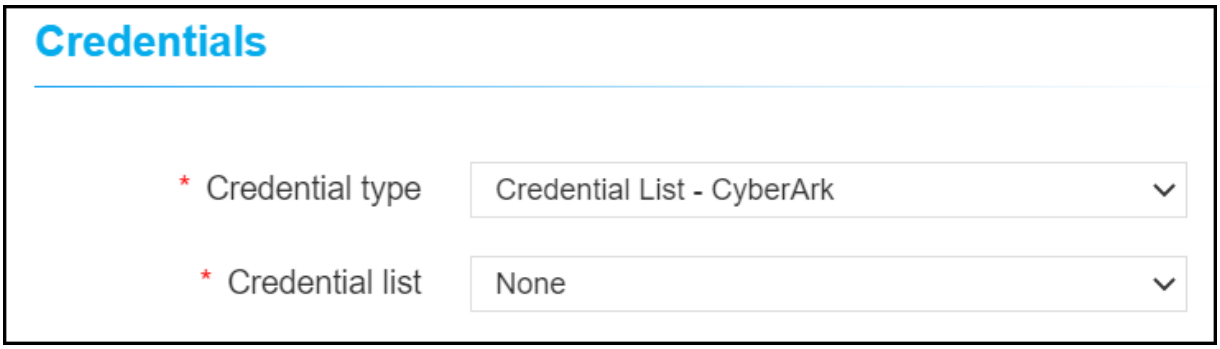
5. Enter or select the field information in the **General information** section.



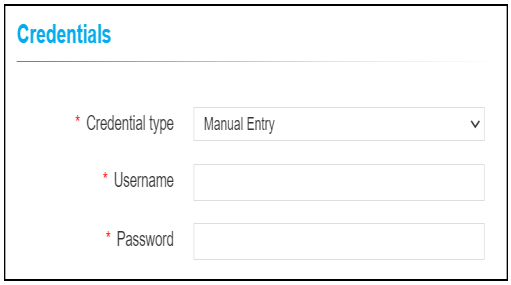
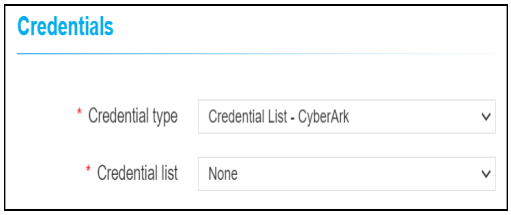
6. The following table provides the field description for adding ADC device details in the **General information** section:

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:

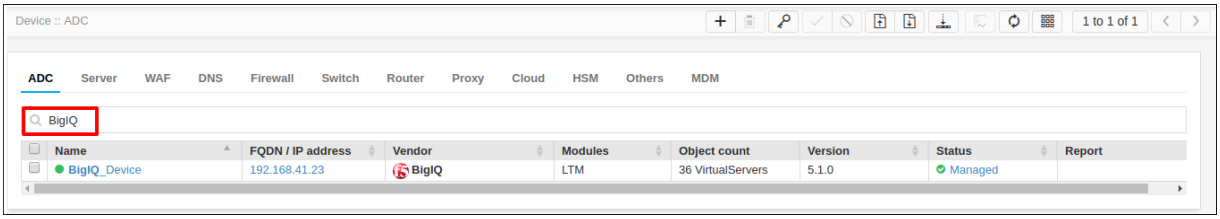
Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page. 	NA
*Username	Text	Yes	Username of the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



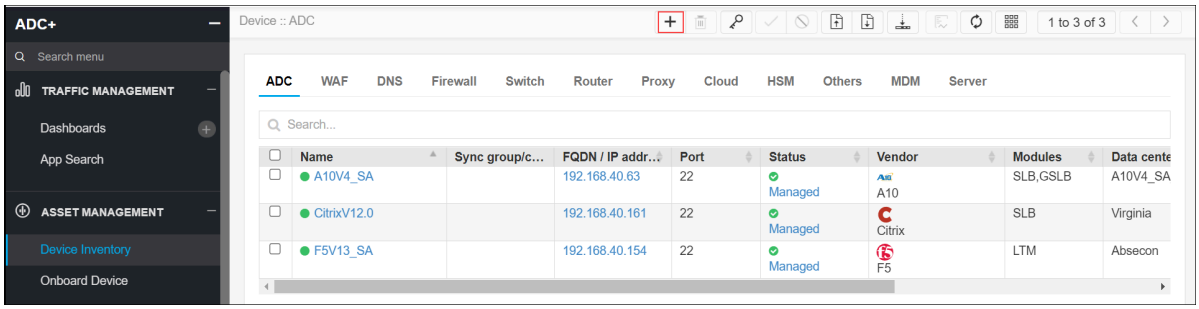
Cisco

- Adding Cisco Device
- Validating the Cisco Device Addition

Adding Cisco Device

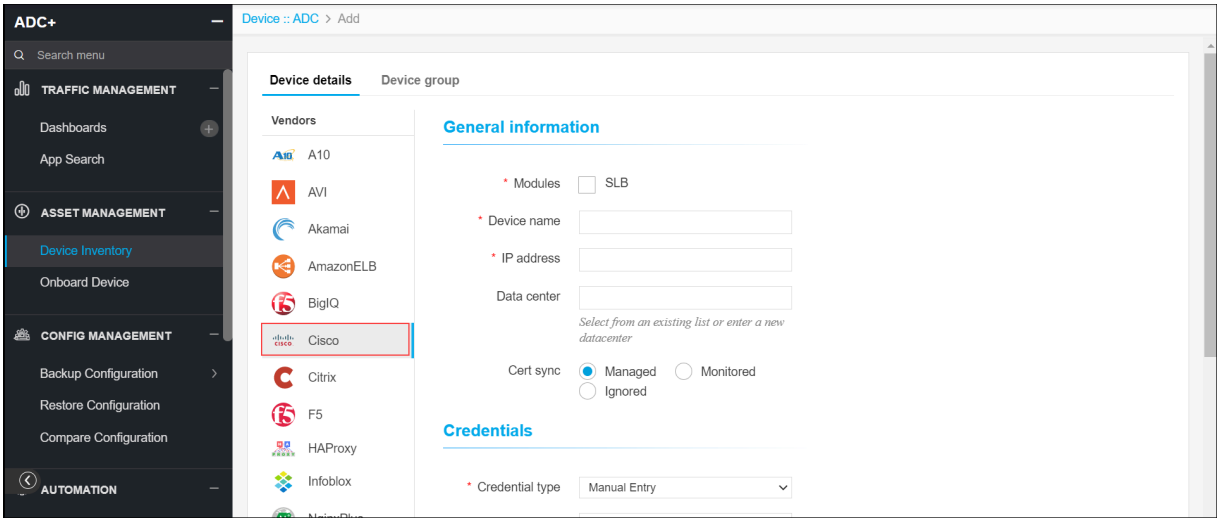
To add Cisco device,

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.

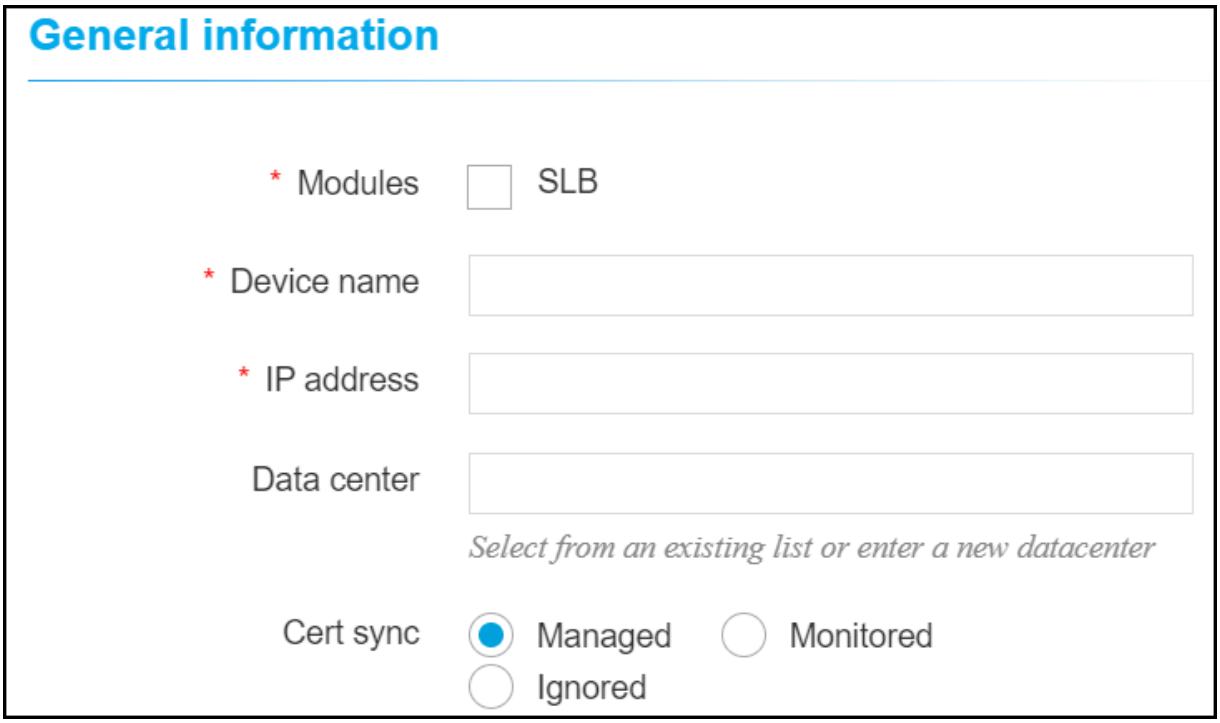


   - Click **Onboard Device** in the left navigation panel.

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



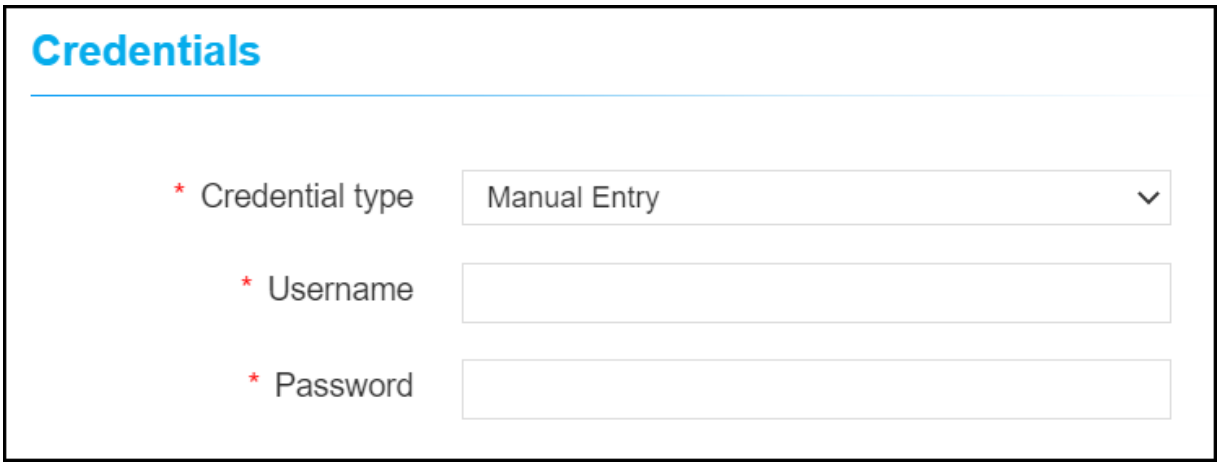
5. Enter or select the field information in the **General information** section.



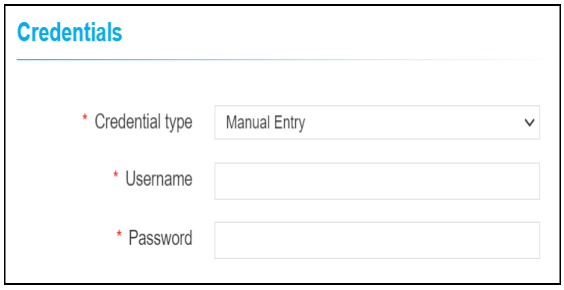
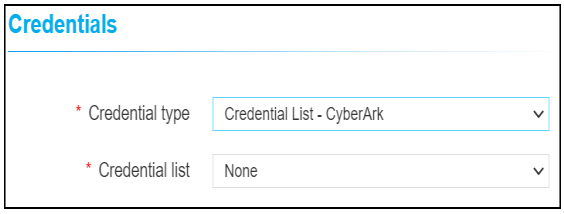
6. The following table provides the field description for adding ADC device details in the **General information** section:

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**: The certificates of the device can be discovered and can only be monitored. **Ignored**: The certificate sync can be ignored.	NA

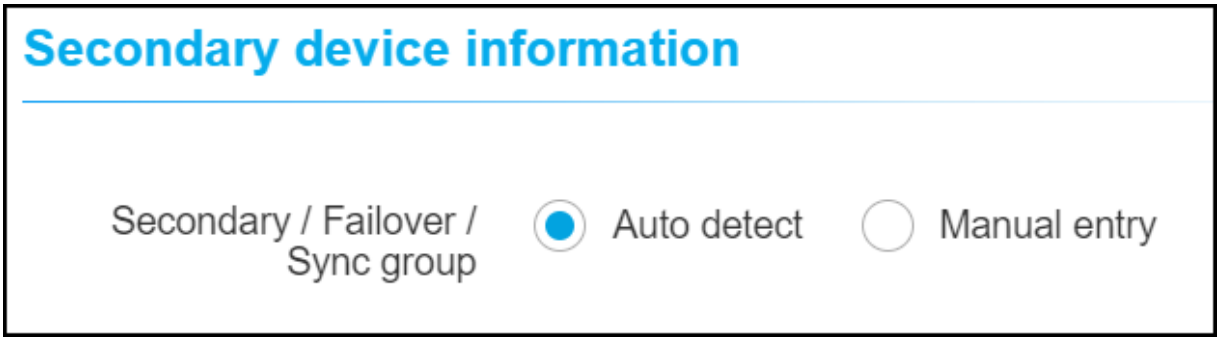
7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



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 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	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:

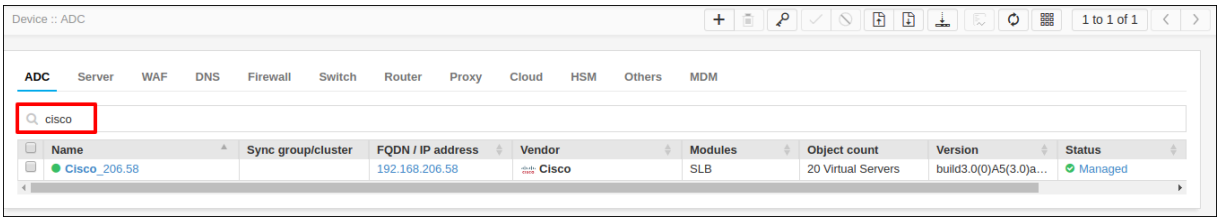
Name	Type	Mandatory	Description	Validation
*Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory. **Manual entry**: The user can use this option to add the peer devices manually.	NA

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.

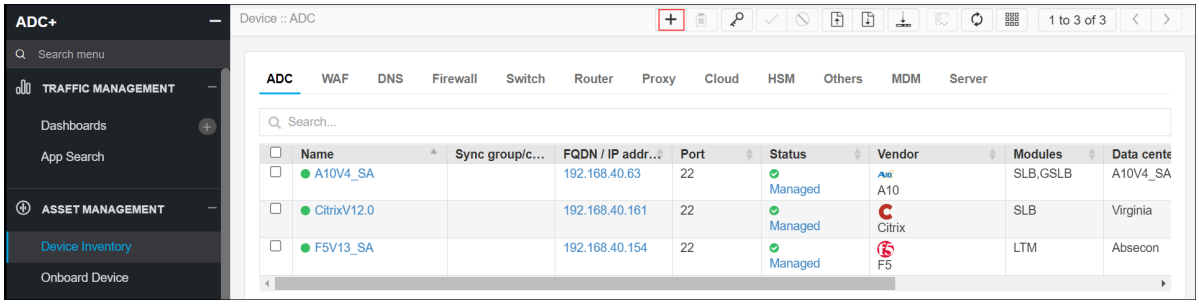


Citrix

Adding Citrix Device

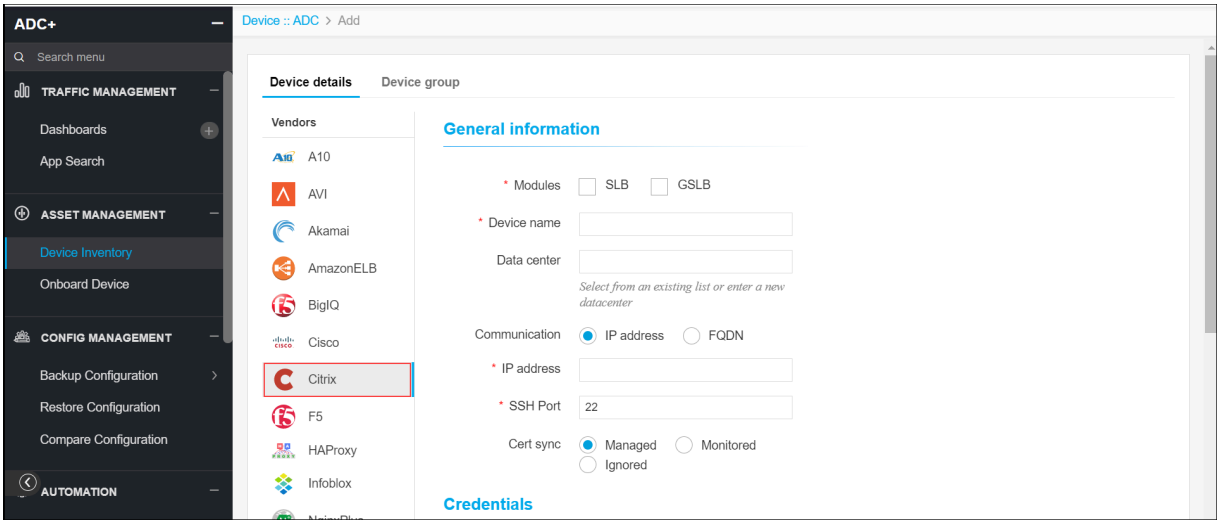
To add Citrix device,

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.

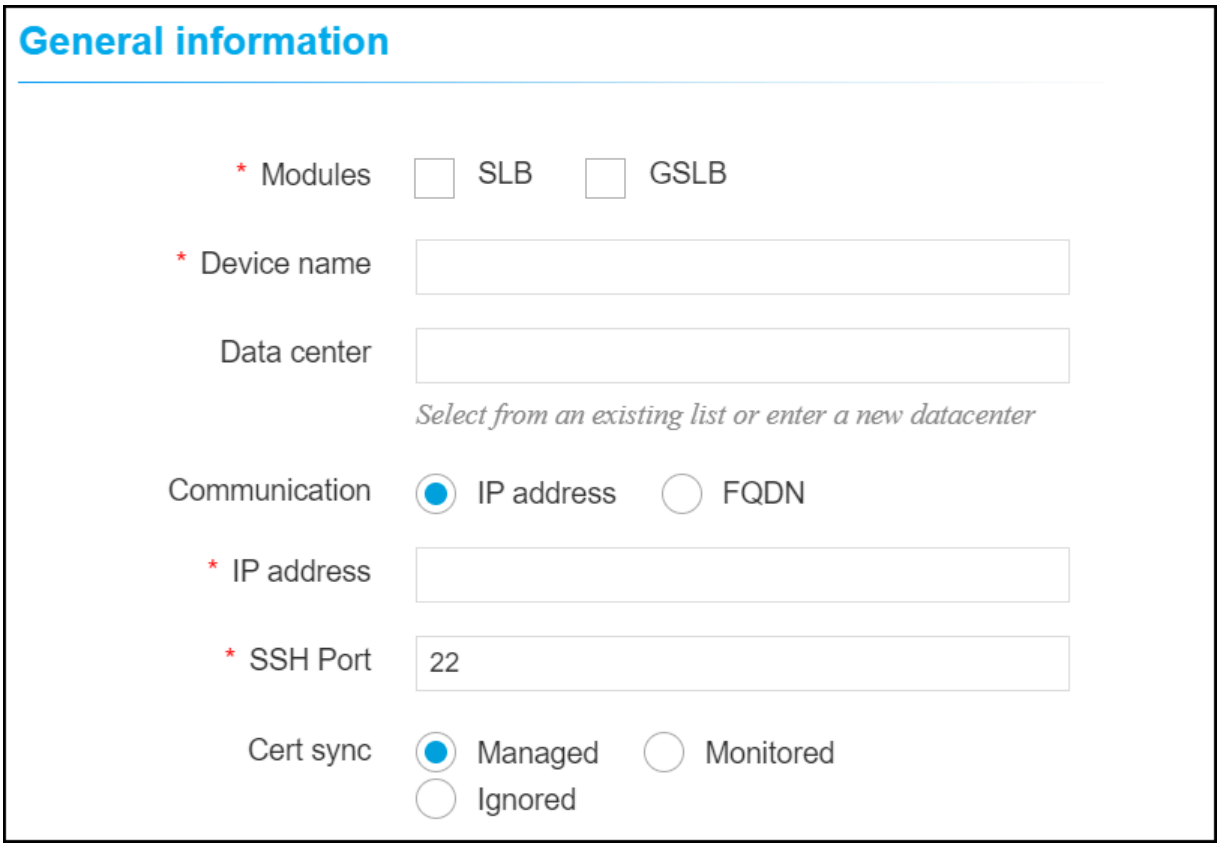


   - Click **Onboard Device** in the left navigation panel.

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



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

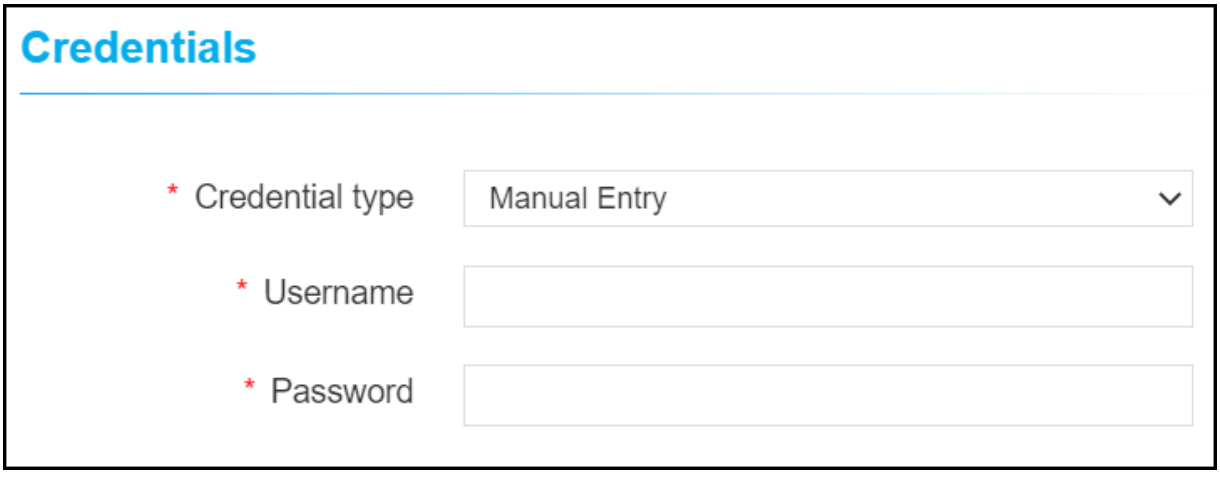


6. The following table provides the field description for adding ADC device details in the **General information** section:

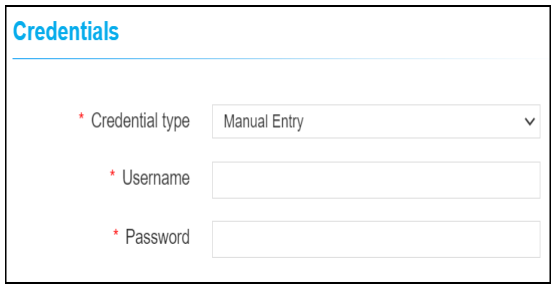
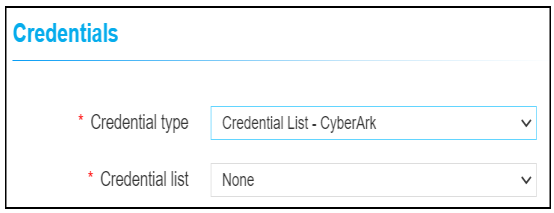
Name	Type	Mandatory	Description	Validation
*Module	Check box	Yes	SLB / GSLB Module.	NA
*Device name	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' and spaces.

Name	Type	Mandatory	Description	Validation
*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

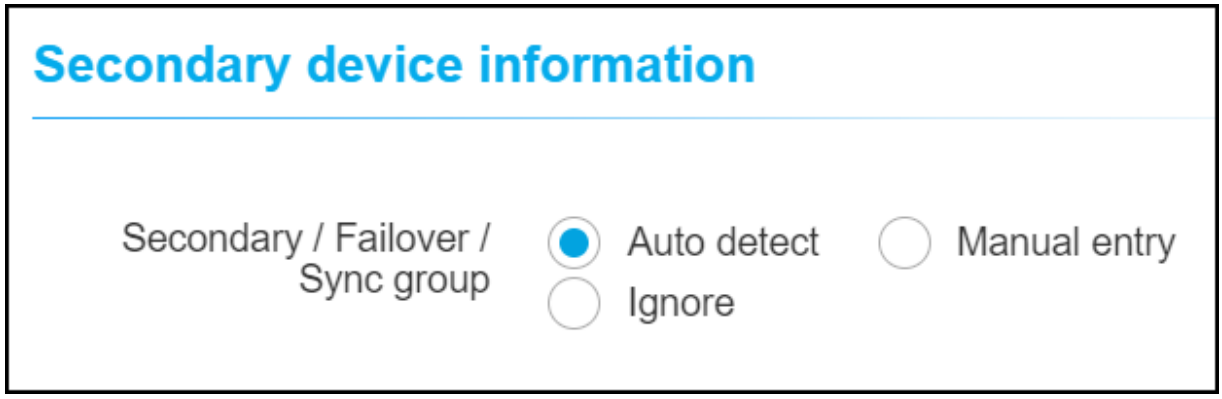
7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



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:

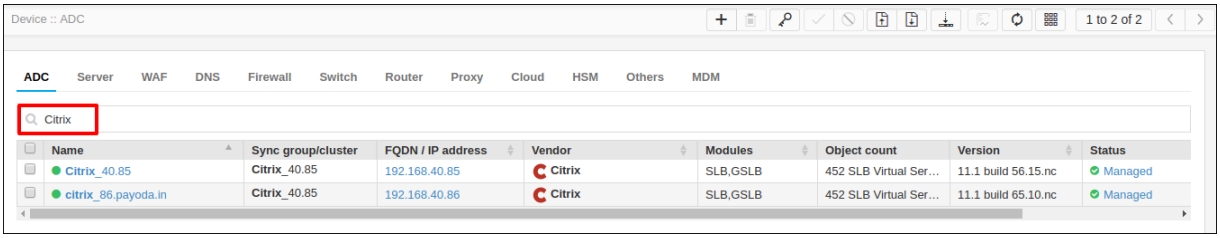
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The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



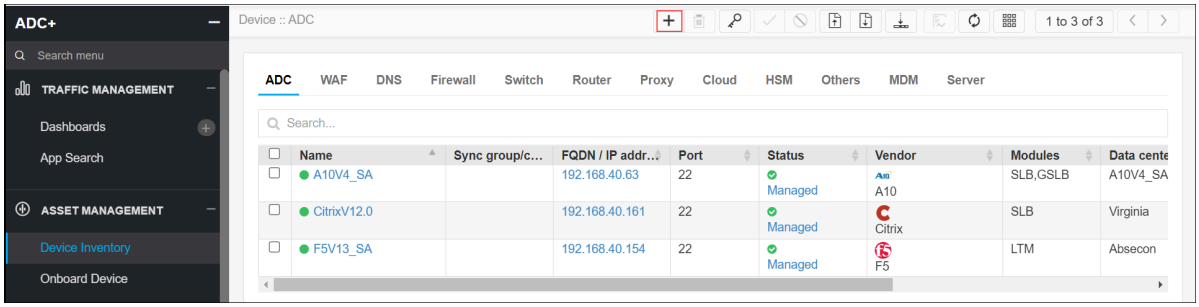
F5

- Adding F5 Device
- Validating F5 Device Addition

Adding F5 Device

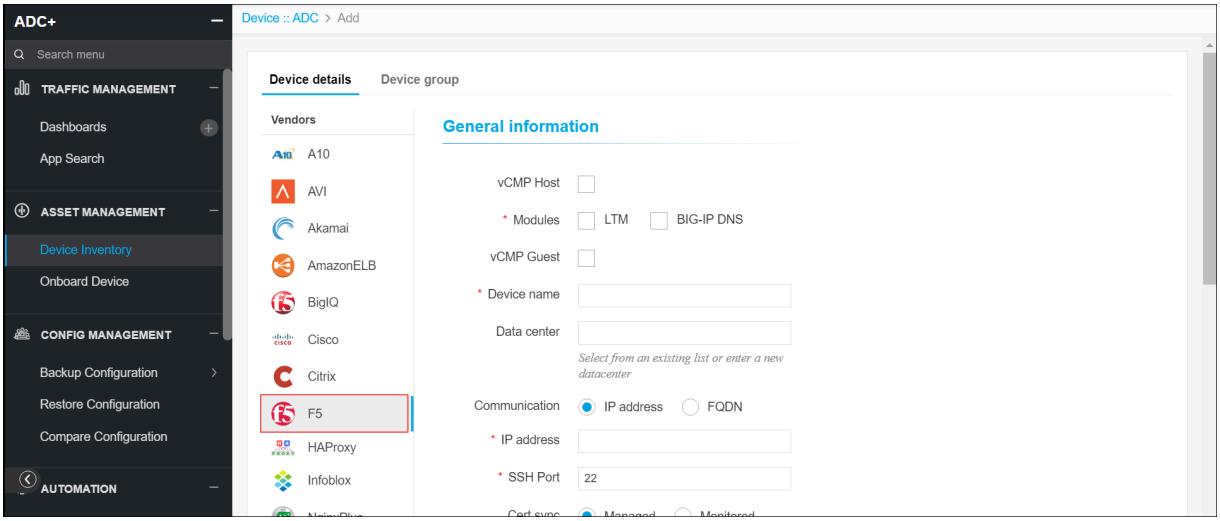
To add F5 device,

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.

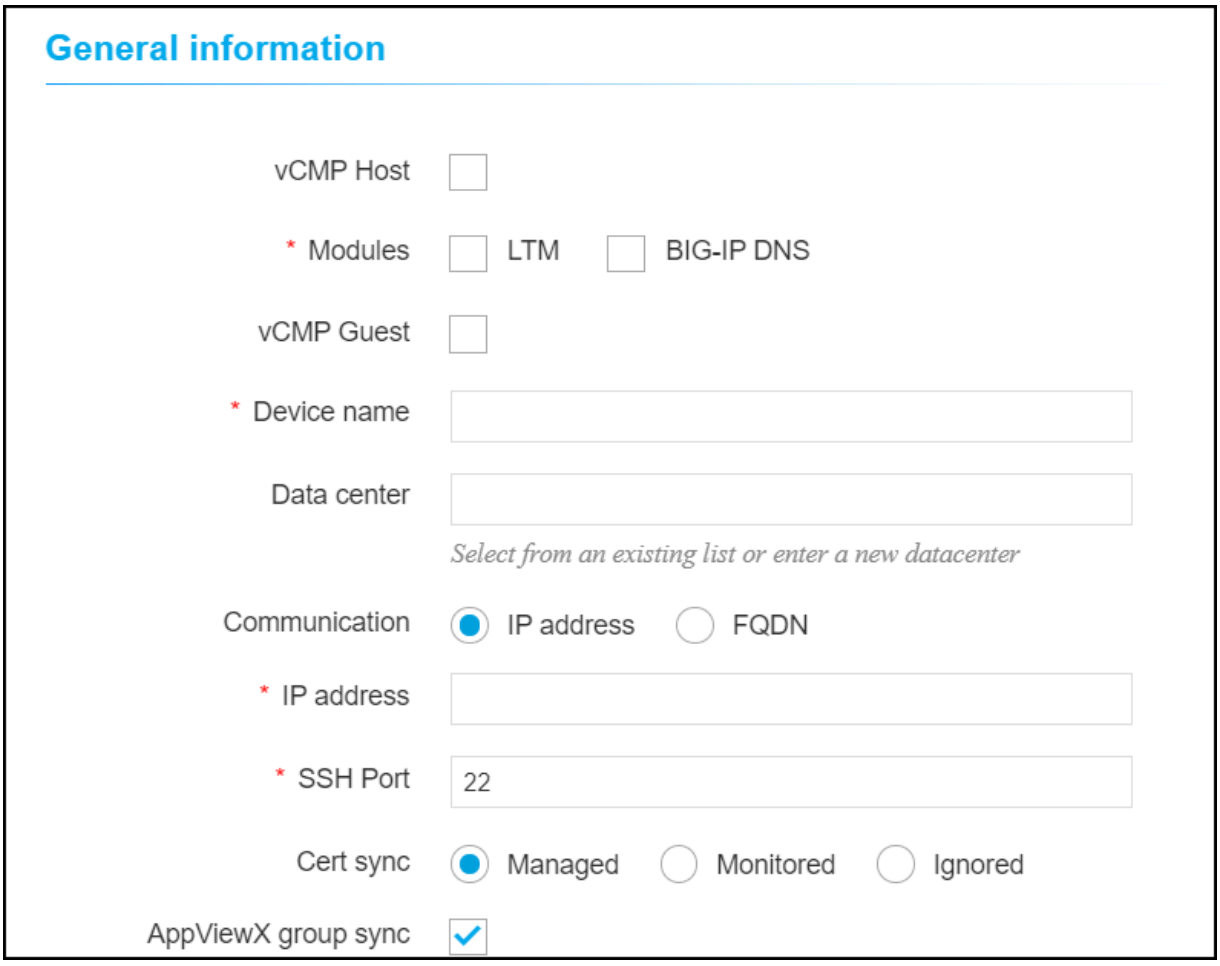


   - Click **Onboard Device** in the left navigation panel.

4. In the **Device details** page, click on the **F5** icon.



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

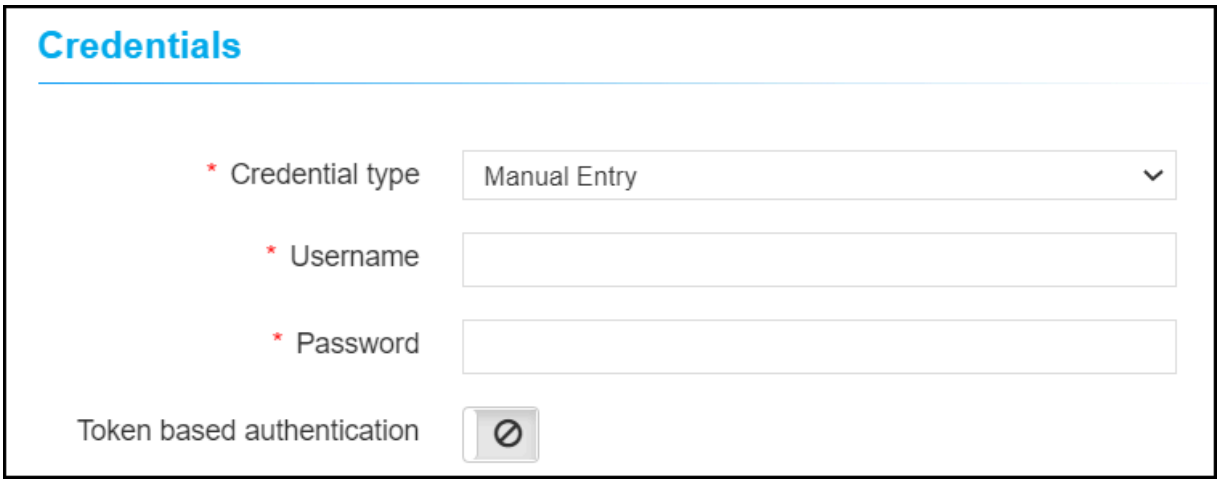


6. The following table provides the field description for adding ADC device details in the **General information** section:

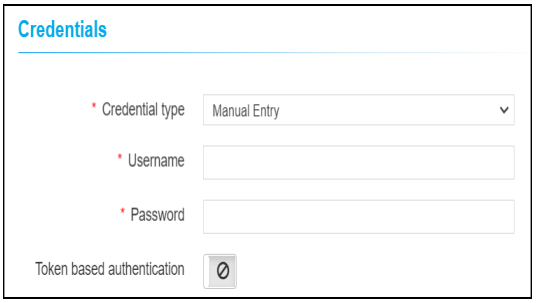
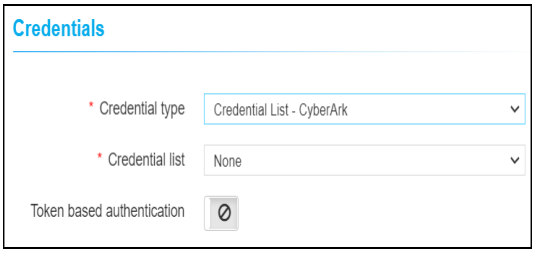
Name	Type	Mandatory	Description	Validation
VCMP Host	Check box	No	To add a device as a vcmb host, this checkbox should be checked.	NA
*Module	Check box	Yes	LTM / BIG-IP DNS Module.	NA
VCMP Guest	Check box	No	To add a device as a vcmp guest, this checkbox should be checked.	NA

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	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**: 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 **Credentials List**.

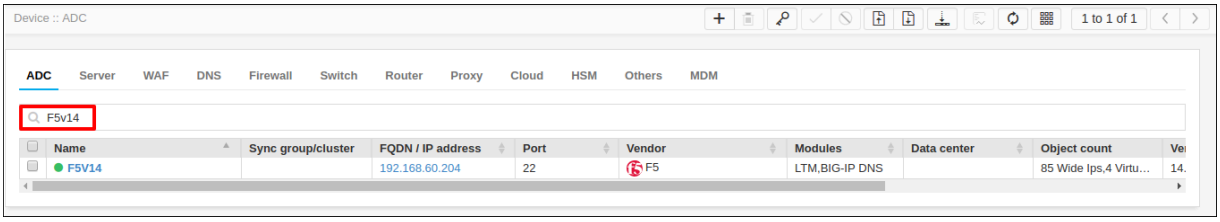


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

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. For more details on secure authentication, refer to Platform User Guide.  	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
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:

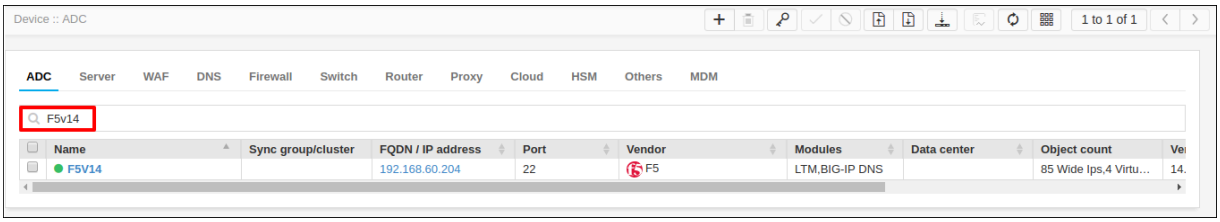
Name	Type	Mandatory	Description	Validation
Secondary device information	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: The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



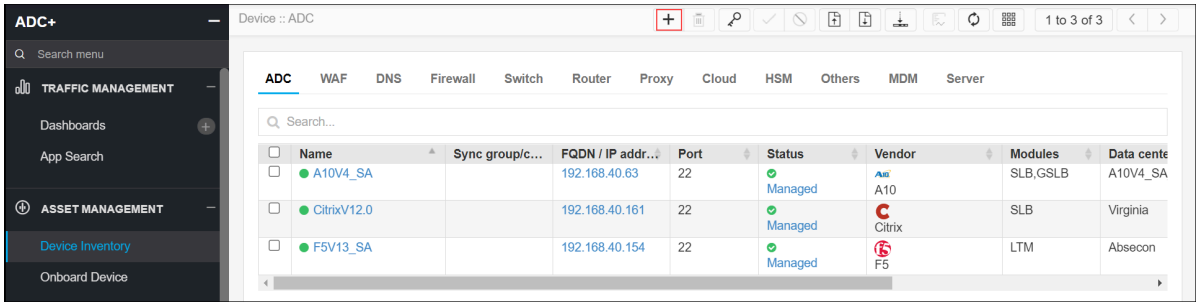
HAProxy

- Adding HAProxy Device
- Validating the HAProxy Device Addition

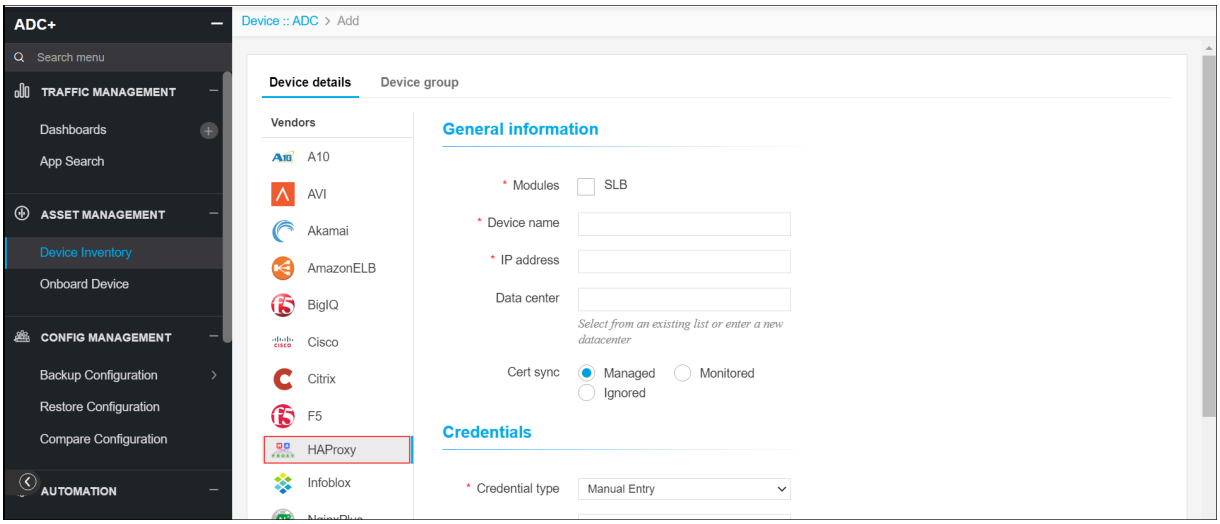
Adding HAProxy Device

To add HAProxy device,

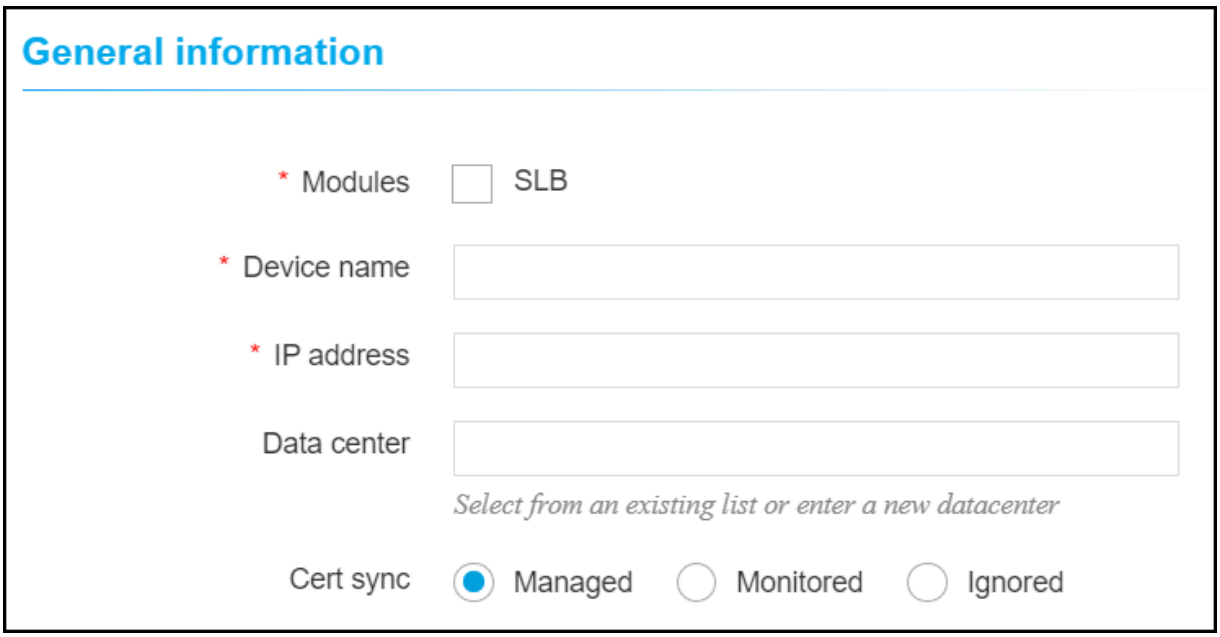
1. Login to the AppViewX application with valid credentials.
2. Go to **Menu** > **ADC+** > **ASSET MANAGEMENT**.
3. Perform any of the following:
   - Click **Device Inventory**, and then select **Add (+)** icon to navigate to the Device details page.



   - 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.

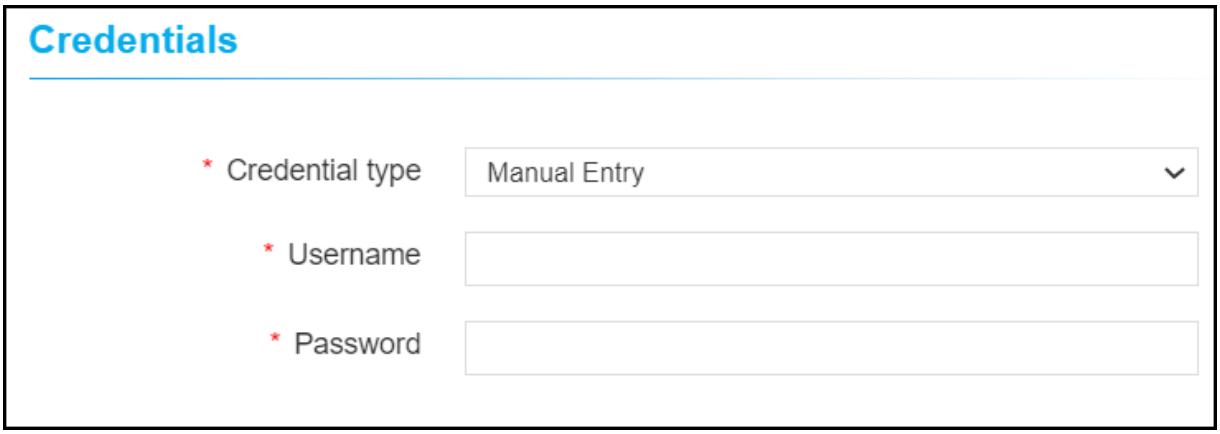


6. The following table provides the field description for adding ADC device details in the **General information** section:

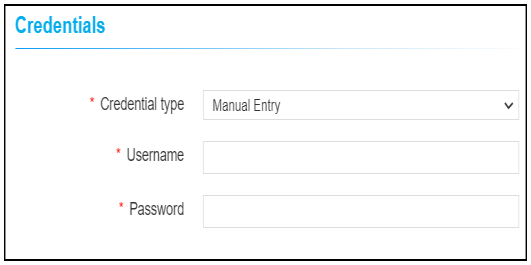
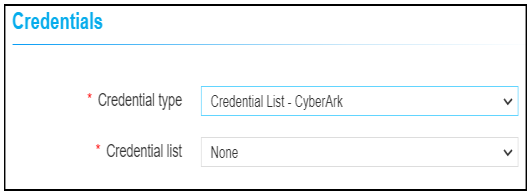
Name	Type	Mandatory	Description	Validation
Device name *	Text	Yes	Unique name of the device to be added.	Device names can only contain alphanumeric characters, '-' , '_' , '.' , '*' , '|' , '!' and spaces.

Name	Type	Mandatory	Description	Validation
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: 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:

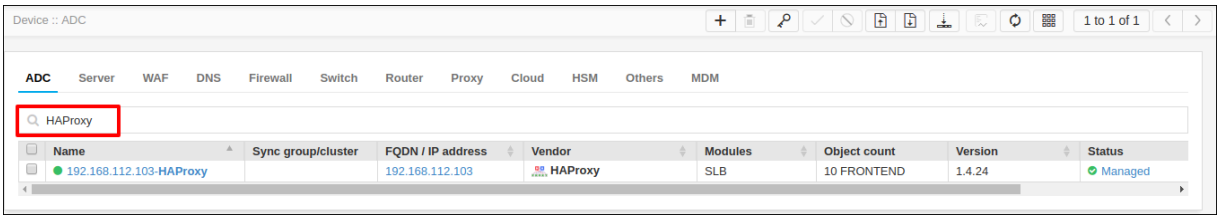
Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	**Manual entry**: The user should enter the username and password.  **Credential List**: The user can select the credential details which are already stored in the credential inventory page.  	NA
*Username	Text	Yes	The user name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

9. 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.

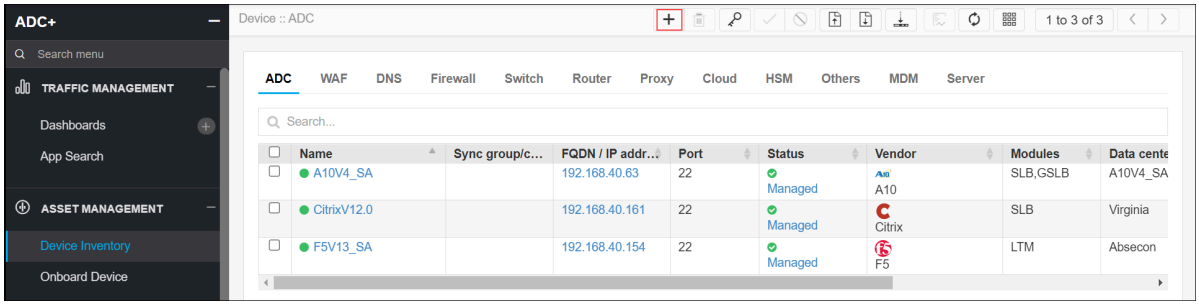


InfoBlox

Adding InfoBlox Device

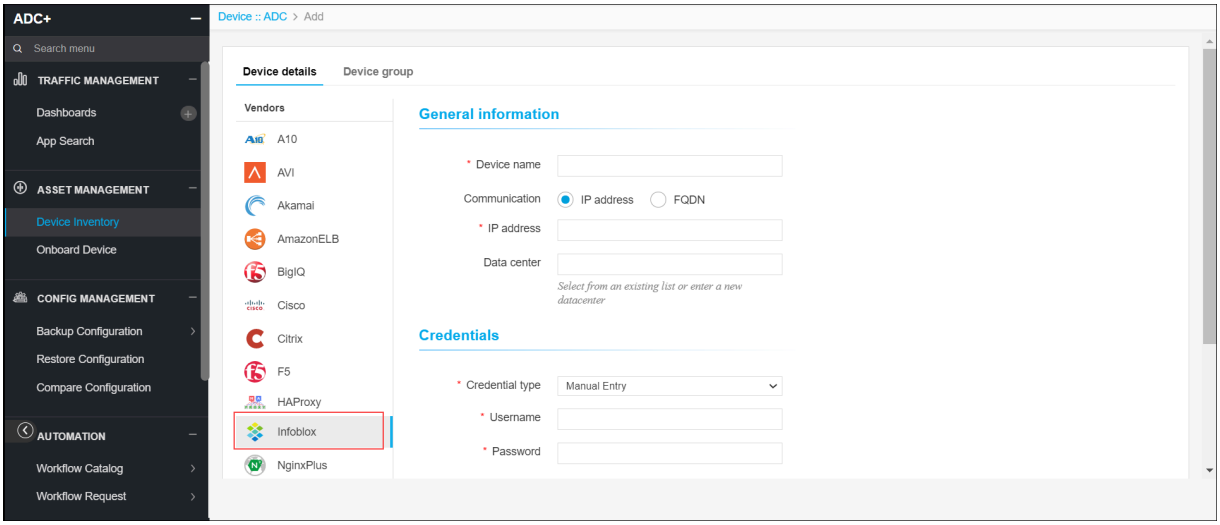
To add InfoBlox device,

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.

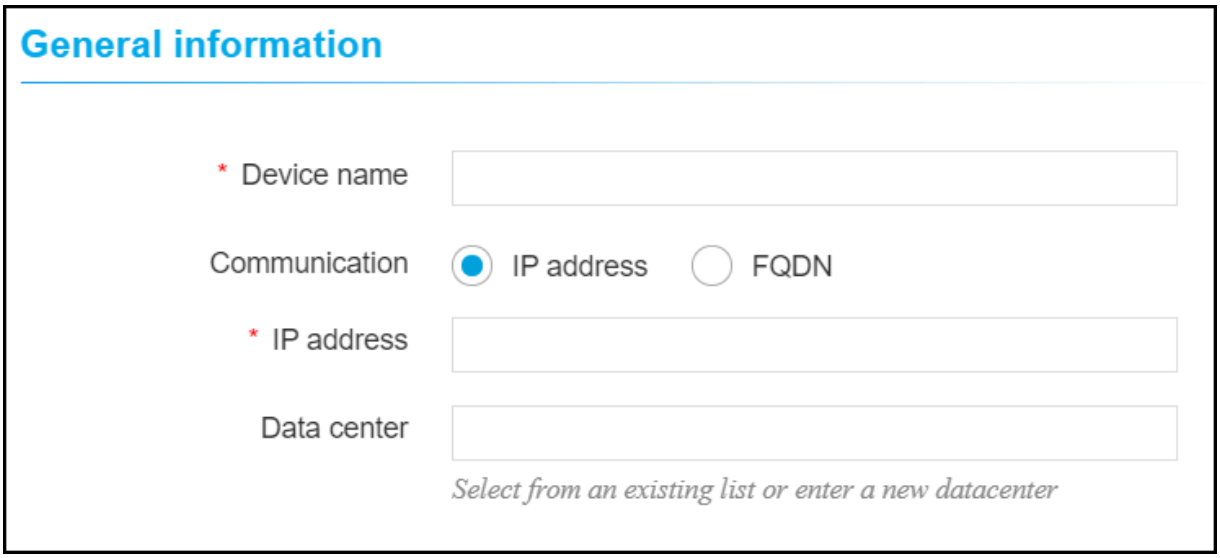


   - Click **Onboard Device** in the left navigation panel.

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



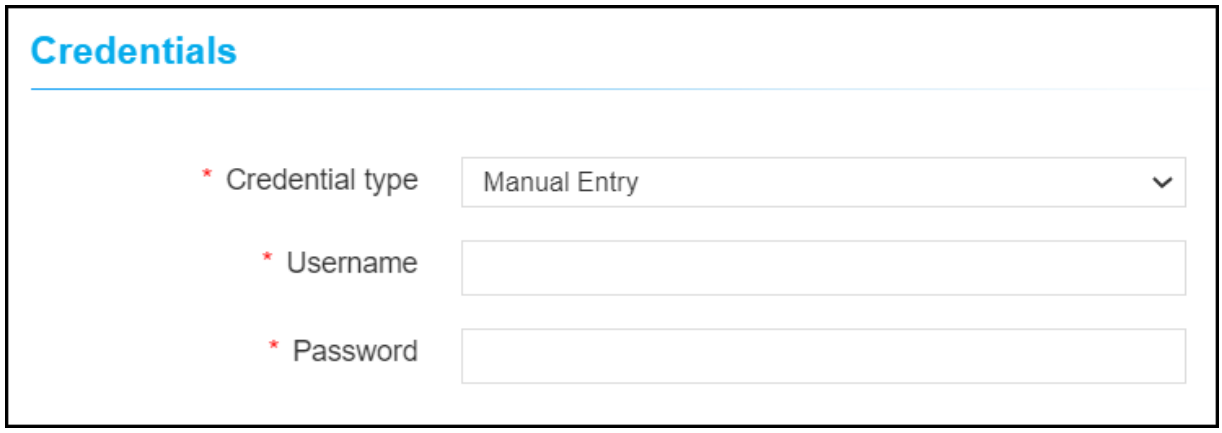
5. Enter or select the field information in the **General information** section.



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.

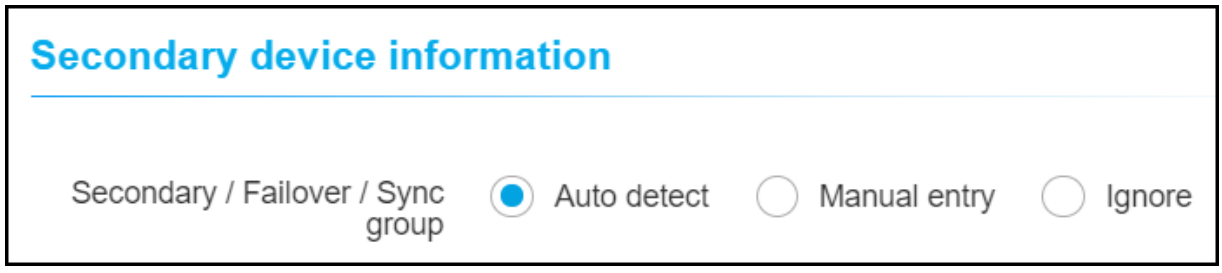
7. Enter or select the field information in the **Credentials** section. You can select **Manual Entry** or **Credentials List**.



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:

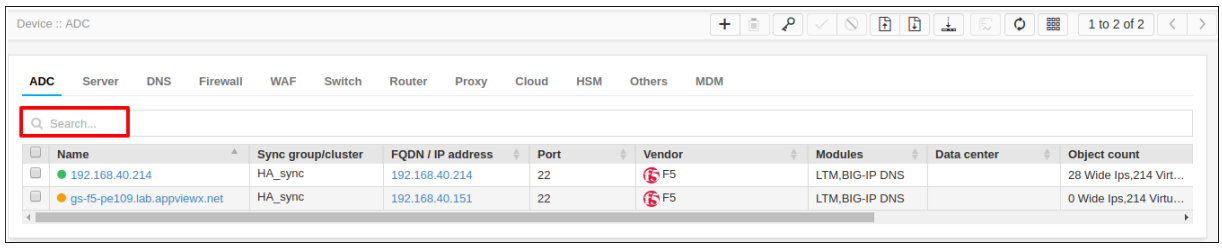
Name	Type	Mandatory	Description	Validation
Secondary / Failover / Sync group	Radio button	Yes	**Auto detect**: The user should select this option to auto-detect and add the peer devices in the inventory page. **Manual entry**: The user can use this option to add the peer devices manually. **Ignore**: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



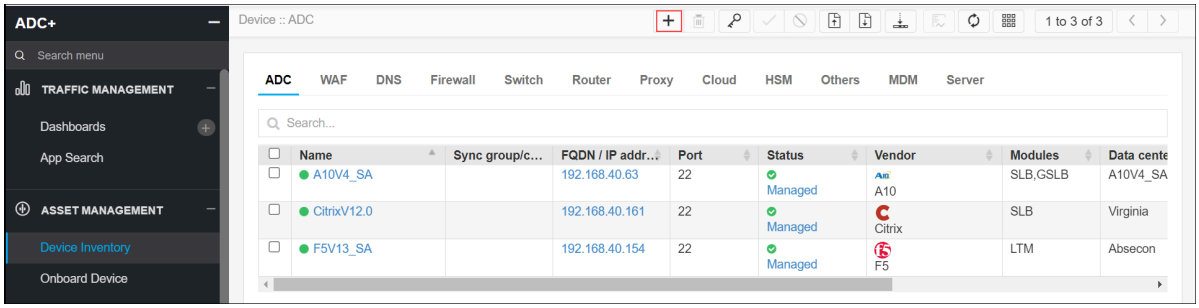
NginxPlus

- Adding NginxPlus Device
- Validating the NginxPlus Device Addition

Adding NginxPlus Device

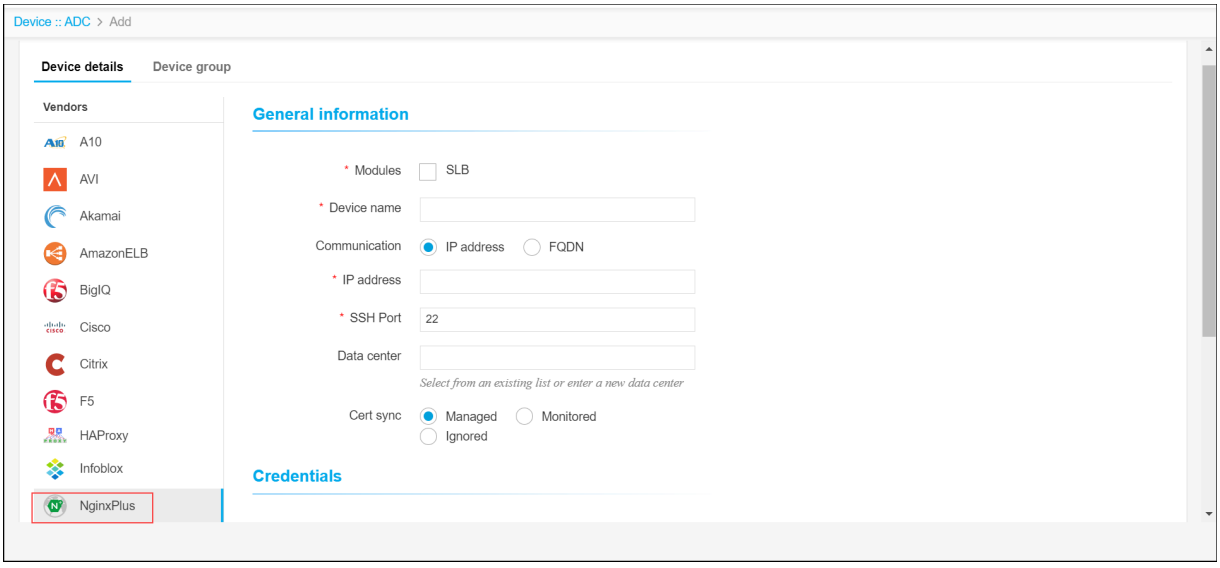
To add NginxPlus device,

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.

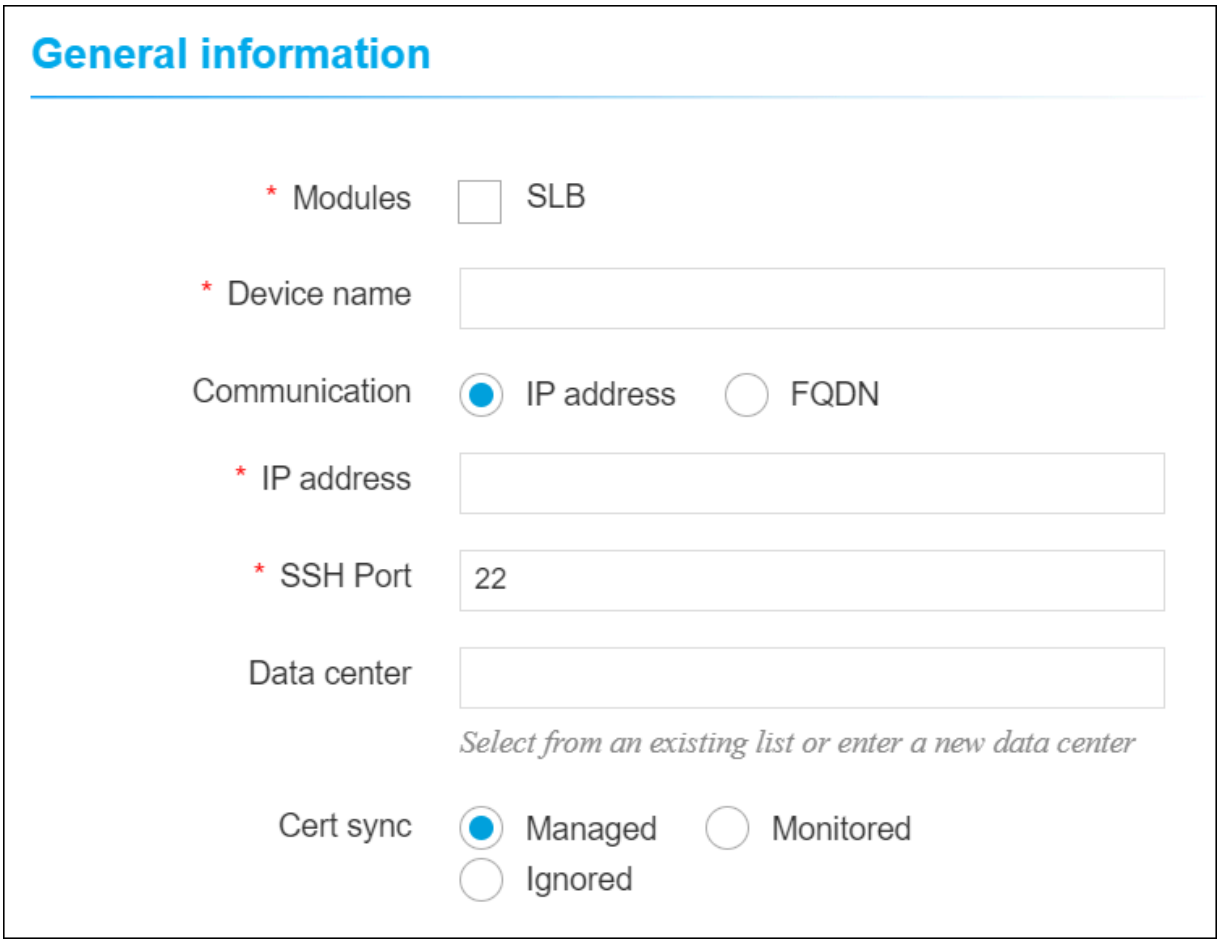


   - Click **Onboard Device** in the left navigation panel.

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



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

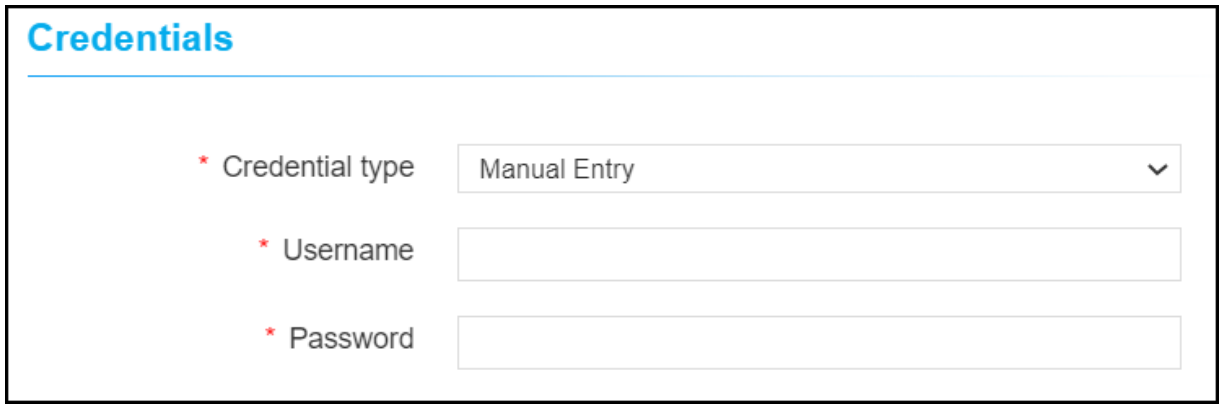


6. The following table provides the field description for adding ADC device details in the **General information** section:

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.

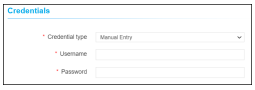
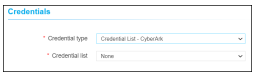
Name	Type	Mandatory	Description	Validation
SSH Port*	Text	Yes	Communication port of the device.	Numbers only.
Data center	Text	No	Datacenter name where the device is configured. The default value is Absecon.	Data center name can only contain alphanumeric characters, '-' , '_' , '.' , '*' , ':' , '|' 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**.

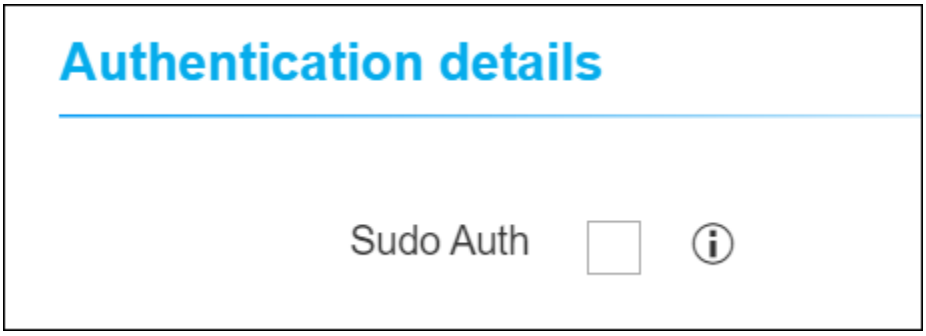


8. The following table provides the field description for adding ADC device details in the **Credentials** section:

Name	Type	Mandatory	Description	Validation
*Credential type	Dropdown	Yes	Manual entry:	NA

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

9. If required, select the **Sudo Auth** checkbox in the **Authentication details** section to enable the Sudo authentication for a non-root user credentials.

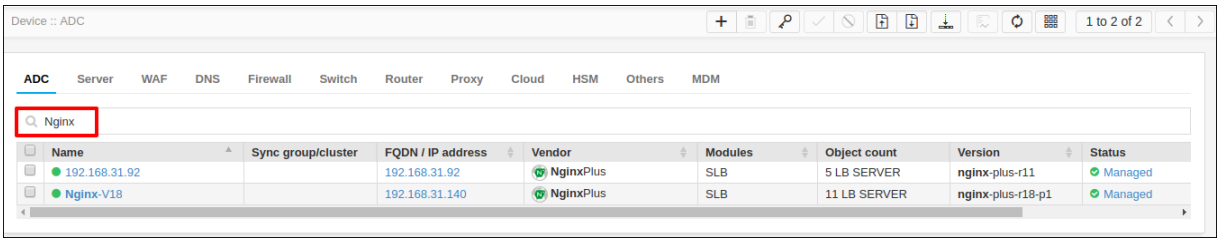


10. Click **Save**.

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 Group

- Group Overview
- Add an ADC Group
- Modify an ADC Group
- Delete an ADC Group

Group Overview

Device group functionality enables categorizing the ADC devices as per custom demands. For example, ADC devices can be grouped based on business units, data centers, global locations, users, or custom needs. This will be helpful in accessing devices of similar types. These custom device groups are efficiently used while scheduling group-based backups and configuring a Heatmap Widgets for monitoring health and triggering automation changes.

Add an ADC Group

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.

Modify an ADC Group

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.

Delete an ADC Group

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.

Chapter 4: CONFIG MANAGEMENT

- Backup Configuration
- Restore Configuration
- Compare Configuration

Backup Configuration

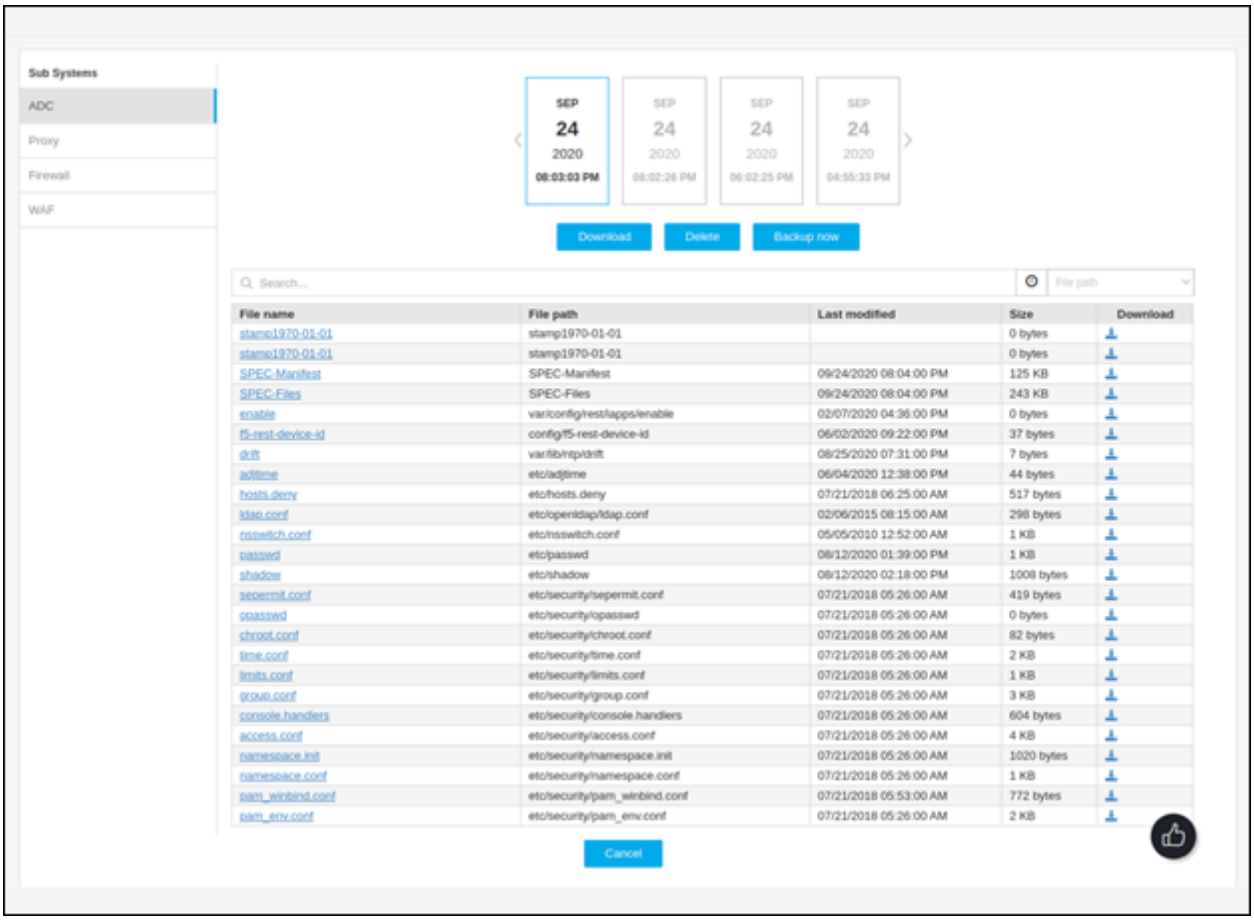
Overview

Manage the complete backup of your devices stored in a central repository in AppViewX. Define your own groups as per the business unit or data center and scheduled backups as needed.

The Backup groups are listed with the devices and their respective archives (with timestamp). Click on the device name to get into the details - A detailed Archive management screen appears that allows you to do the following:

- Click on the Archive to view the file/config within the archive.
- Download the complete archive or individual files.

- Delete the selected archives
- Generate Instant backup



Backup Configuration Management - Overview

Application Delivery Controller solution enables periodical backups to be done on a manual basis or with a scheduling system, which ensures that the entire config archives of all devices are added and managed in a central repository with AppViewX. Along with the ability to perform the backup, you can also restore the archive back to the device either complete archive of device or object level (Virtual Server, Wideip, Monitor, policy, etc.) based on the requirement (for example, restore only one virtual server that was misconfigured during modifications).

Benefits of Configuring Backup

- Ability to compare between two archives to see exactly what changes have taken place between the time frame of archive 1 (vs) archive 2.
- Essential details can be viewed and downloaded as pdf such as the files within the backup folder bigip, conf, etc. for your reference
- If the backup is scheduled on a regular basis, whatever misconfigurations or misbehavior of network outage or power failure on the device can be recovered and restored for valid configuration data.
- Manage your network configuration by automating the backups, track and report network changes and ensure they are compliant with the defined policies.
- Audit the configuration drift and prevent unauthorized or unwanted changes by comparing the configuration across devices visually and restore the changes to adhere to the standards.

Create a Device Backup Group

A device backup group is a container used to store all of the backups and restore records for a particular group within the AppViewX system.

To create a device backup group,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Create Backup**. The **Create** screen opens.

   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 backup 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 backup group if the devices match the search criteria you set up.

2. Enter a name for the backup group.
3. (Recommended) Enter a description of the group that makes it easy for users to determine what sort of device backups are found within the group.
4. Select the **Device** or **Device Group** radio button based on how you want to define the device backup.
5. In the Available devices field, click the » (**Assign item**) icon beside each device whose backups and restores you want to include in the group.

6. In the **scheduling** field, select either the **Scheduler** radio button and then set the frequency, starting date, and time for the backups, or select the **Generate** now radio button to start the backup as soon as you click Save.
7. In the **Email configuration** field, enter the email addresses, separated by commas, of all users who should be sent a copy of the backup.
8. (Recommended) Enter a short, clear description in the **Subject** field so that it will help the recipients understand why they are receiving the email: for example, "Weekly backup of ADC devices."
9. Click **Save**.

> **Note:** You can customize the archive count for storing the daily, weekly, monthly, and yearly backups individually. Using this feature, you can maintain scheduled archives without it being overwritten by instant backups.

Delete a Device Backup Group

To remove a device backup group from the AppViewX system,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Manage Backups**.
   The **Backup** tab opens.
2. Click the (**Delete**) icon against the device backup group that you want to delete.
   The Confirmation pop-up opens.
3. In the Confirmation pop-up, you have an option to enable Retain the generated backups. This option is enabled by default.

> **Note:** The retained backups will be moved to the Default group for later references.

4. Click **Yes** to confirm that you want to delete the device backup group.

> **Note:** To discard the deletion, click **No**.

Edit the Details of a Backup Group

To edit the details of a device backup group,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Manage Backups**.
   The **Backup** tab opens.
2. In the list of backup groups on the screen, click the (**Edit**) icon for the device backup group you want to modify.
   The **Modify** screen opens.
3. In the **Modify** screen, update description, add/remove devices, change scheduler interval, and Email options.
4. Click **Save**.

Initiate Instant Device Backup

A device backup group is a container used to store all of the backups and restore records for a particular group within the AppViewX system.

To create an instant device backup group,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Manage Backups**.
   The **Backup** tab opens.
2. If the **Backup** tab is not displayed by default, click to open it.
3. In the list of backup groups on the screen, click the (**Expand**) icon for the device you want to back up immediately.
4. Click the **Device name** link in the table that appears.
5. On the **Archive details** screen that appears, click **Backup Now**.

Schedule a Device Backup

To schedule a device backup,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Manage Backups**.
   The **Backup** tab opens.
2. Click the **Create** button in the Command bar.
3. On the **Create** screen that opens, enter a name for the backup you are about to schedule.
4. (Optional) Enter a description of the backup.

5. In the **Available devices** field, click the »**Assign** icon beside each device you want to add to include in the backup.
6. Select the **Scheduler** radio button.
7. Depending on how often you want to schedule a backup, select the Daily, Weekly, Monthly, or Yearly radio button.
8. Type the starting date of the backup or click the (**Starting date**) icon and select the date from the popup screen that appears.
9. Type the starting time for the backup or click the (**Time**) icon and select a start time using the sliding bars for Hour and Minute. When you are finished, click Done to close the popup screen.
10. (Optional) If you want certain users to be notified of the backup generation status (success or failure) via an email, enter their email addresses separated by commas in the To field of the Email configuration section, then enter a subject that will help the recipients understand why they are receiving the email: for example, "Weekly backup of ADC devices."

> **Note:** Email notifications will be sent for each device within the backup group. The successful backup notification will have the archive attachment in .ucs format via email.

11. Click **Save** to finish scheduling the backup.

> **Note:**
> - Rather than adding components manually, you can click the Add search string link and create a search string that automatically assigns all existing devices that match the search criteria. 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 backup if the devices match the search criteria you set up.
> - The minute bar has only two settings: to the left, representing the top of the hour (:00) and to the right, representing half-past the hour (:30).

View the Backup Schedule for a Device

To view the backup schedule for a device,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Backup Configuration** > **Manage Backups**.
   The **Backup** tab opens.

2. In the **Backup** tab, Hover your mouse over the Calendar icon of the device whose backup schedule you want to view.
3. A popup box appears, listing the frequency, start date, and start time of backups for the selected device.

Note: If a device has no backups scheduled, no calendar icon appears in its row in the device table, as is the case for the a10 device that appears in the image above.

Delete the Backup and Restore History for a Device

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. In the list of backup groups on the screen, click the (**Expand**) icon for the device backup group whose backup and restore history you want to delete.
3. In the table that appears, click the Device Name link for the device whose history you want to delete.
4. On the **Archive details** screen that appears, click the **Delete** button.
5. On the popup screen that appears, click **Yes** to confirm that you want to delete the backup and restore history for the device group.

Download the Backup and Restore History for a Device

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. In the list of backup groups on the screen, click the (**Expand**) icon for the device backup group that contains the device whose history you want to download.

3. In the table that appears, click the Device name link for the device whose history you want to download. The Archive details screen appears, listing all of the back-ups and restore events for the device.
4. Perform one or both of the following download actions:
   - Scroll through the date range at the top of the screen, click on a specific date, then click the Download button to download all backup and restore events that occurred on that date for the device.
   - Use the search field and calendar filter to locate specific backups or restore events based on filename, file path, or date range, then click the (**Download**) icon for each result you want to download.

View the Backup and Restore History for a Device

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. In the list of backup groups on the screen, click the (**Expand**) icon for the device backup group that contains the device whose history you want to view.
3. In the table that appears, click the Device name link for the device whose history you want to view.
4. The Archive details screen appears, listing all of the back-ups and restore events for the device.
5. (Optional) Use the search field and calendar filter to locate specific backup or restore events based on filename, file path, or date range.

Edit the Settings of the Backup Screen

The device backups are referred to as Archives. Customize the Archives limits per device (maximum of 80 archives per device can be configured) through the customization option. Upon crossing the limit, the oldest archive will be overwritten automatically. You can also distribute the archive count against Daily, Weekly, Monthly, and Yearly flags so that scheduled archives are not overwritten soon. Save the changes upon configuration.

To edit the settings of the Backup screen, complete the following steps:

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. In the Sub Systems column on the left, click ADC (default tab).
3. Click the (**Settings**) button in the Command bar.

4. On the Settings popup screen that appears, select the number of archives you want to keep for each device: you can choose to keep anywhere from 1 to 80.
5. Select the Display warning messages when overwriting the archives checkbox if you want users to be warned whenever they are about to overwrite an archive.
6. Click **Submit** to save the settings.

Restore Configuration

- Restore Configuration - Overview
- Restore and Rollback a Device
- Restore and Rollback an Object

Restore Configuration - Overview

AppViewX allows you to restore configuration backups on ADC devices. It supports device-level to overwrite the complete device config and as well object-level restoration to restore a particular Application that is failing or detected with an unwanted change.

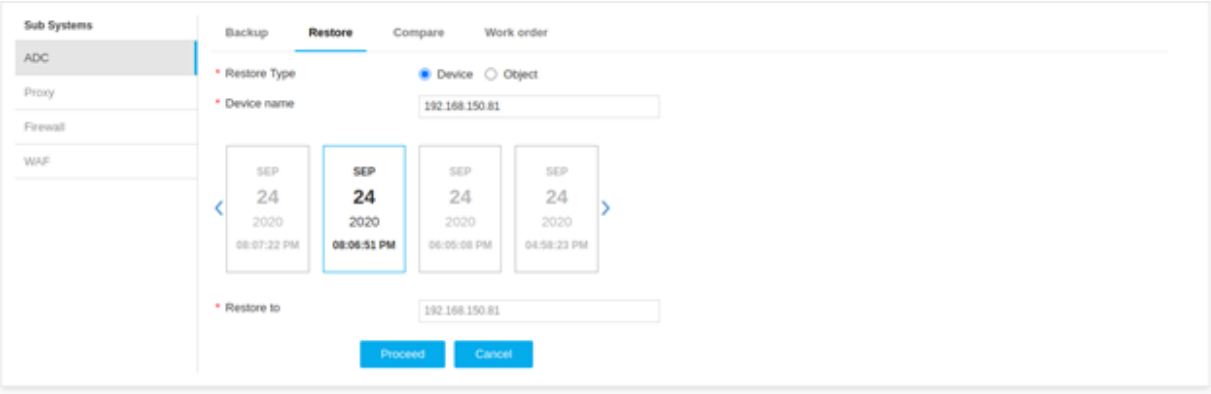
Restore and Rollback a Device

Restore the configuration of the ADC device from current config to a preferred config. AppViewX enables to compare the configuration before proceeding with the restoration. During a restore, AppViewX will take a backup of the current configuration that is to be used during rollback.

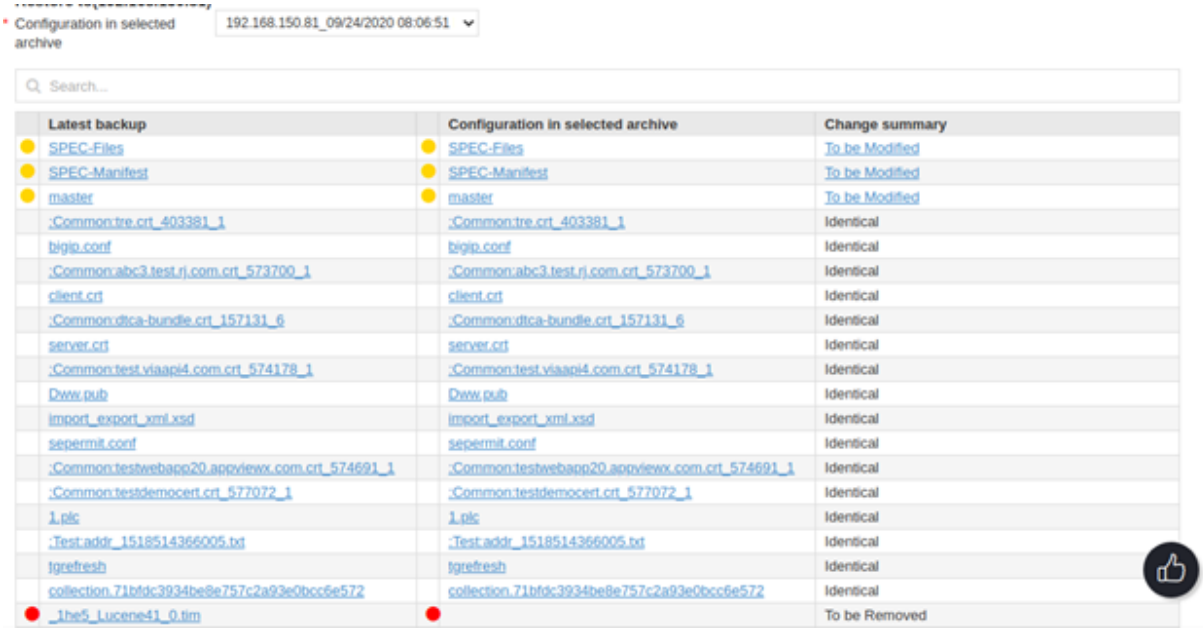
On proceeding with restore, a Work order will be generated in AppViewX to track progress. On a successful restore, required configurations will be updated in the device. In case of failure, an automatic rollback will be initiated by AppViewX.

To restore a device, complete the following steps:

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. Select the **Restore Type**: Device.
3. Enter the **Device name**.
4. In the date range field that appears below the **Device name** field, click the date you want to restore the device or object to.
5. Leave the default value in the **Restore to** field.



6. Click **Proceed**.
7. The screen refreshes and displays a Configuration in the latest archive field, which should show the backup you selected. The table below shows all of the files contained in the backup and displays yellow circles beside each file that has been modified since the backup was taken and red circles beside each file that has been removed since the backup date.



8. At the bottom of the screen, enter a reason for restoring to the backup.
9. Click **Restore**.
10. Validate the changes against the latest backup and the configuration that is going to be restored. Enter a reason for restore and proceed.
11. AppViewX will proceed with restoring the entire configuration file or the particular configuration of the objects in a step-by-step manner.

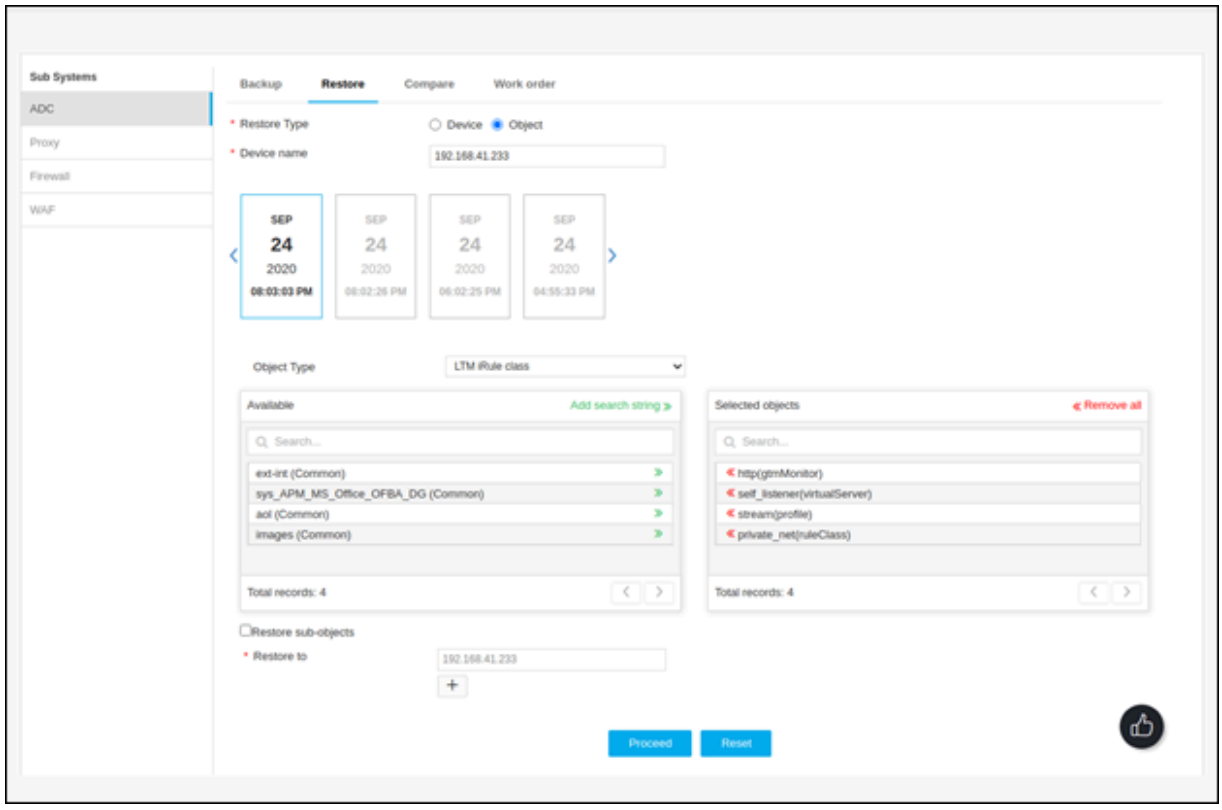
12. A Work Order ID will be generated to track the progress at anytime. (Track the IDs in the Work order tab)
13. During restoration, if AppViewX identifies any issues, an automatic configuration Rollback will be triggered, which can be tracked in the work order.
14. A manual Rollback can also be initiated on a need basis.

Restore and Rollback an Object

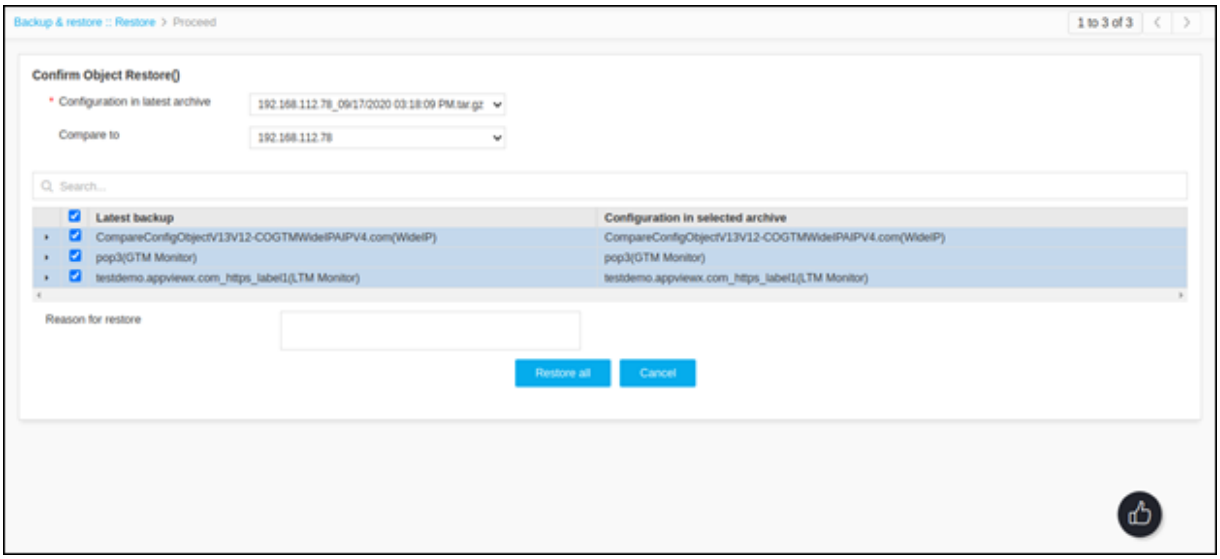
Restore one or more Application services configurations from the current config to a preferred config and apply it on multiple devices. AppViewX enables to compare the configuration before proceeding with the restoration. During the restoration, the complete hierarchy of the selected object(s) will be restored in a step-by-step manner. AppViewX will consider the recent device backup as the source to roll back the configurations. On successful restore, configurations will be updated in the device. In case of failure, an automatic rollback will be initiated by AppViewX.

To restore an object, complete the following steps:

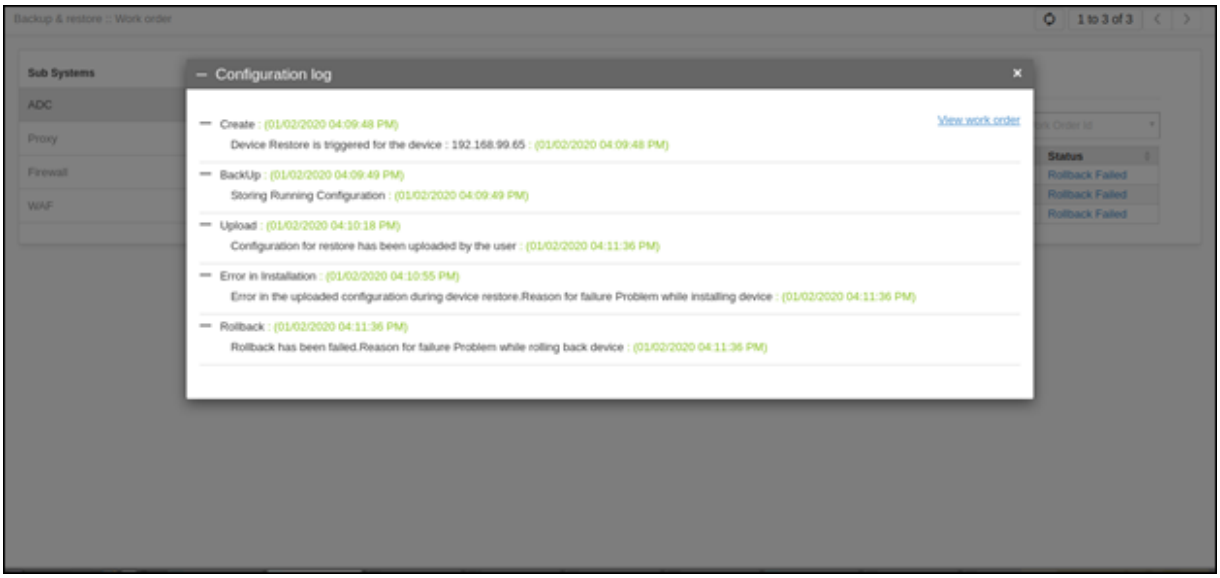
1. Click the  **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Restore Configuration**.
   The **Restore** tab opens.
2. Select the **Restore Type**: Object.
3. Select the Source device, Archive to be used for restore.
4. Select the objects that need to be restored.
5. Select the destination devices (it could be one or more devices), and then click **Proceed**.



6. The screen refreshes and displays a table that compares the latest device backup and the selected archive configuration with change highlighted. Each object can be expanded and viewed:
   - Yellow - Modified line
   - Green - Added line
   - Reg - Deleted line



7. Validate the changes against the latest backup and the configuration that is going to be restored. Enter a reason for restore and proceed.
8. AppViewX will proceed with restoring the particular configuration of the objects selected in a step-by-step manner.
9. A Work Order ID will be generated to track the progress anytime. (Track the IDs in the Work order tab)
10. During restoration, if AppViewX identifies any issues with respect to even one of the objects, an automatic configuration Rollback will be triggered, which can be tracked in the work order.
11. A manual Rollback can also be initiated on a need basis.



Compare Configuration

Compare Configuration - Overview

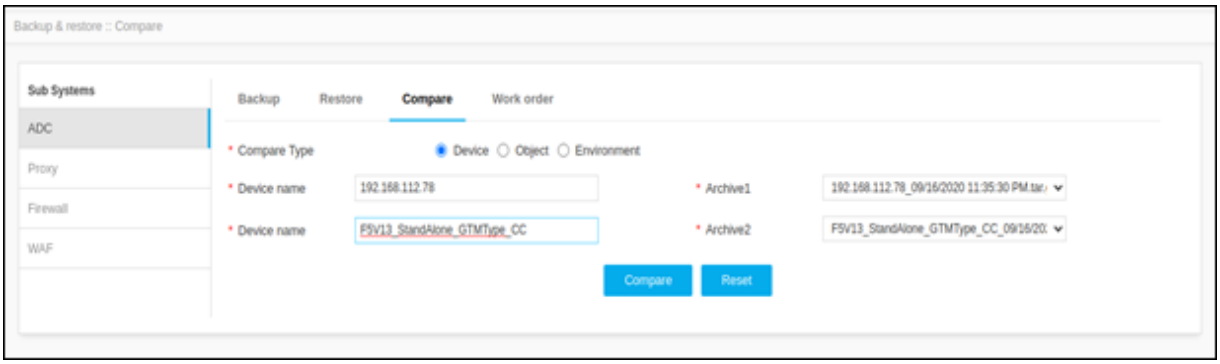
AppViewX platform enables you to compare the complete configuration of load balancers within or across multiple devices through previous backups. It indicates the files that are modified and also provides an option to drill down into the actual configuration change. Ensure the changes are validated and generate reports out of it.

AppViewX allows the configuration to be compared for the entire Device, Specific object within the device, or a custom Environment as per the need.

Compare Device Backups

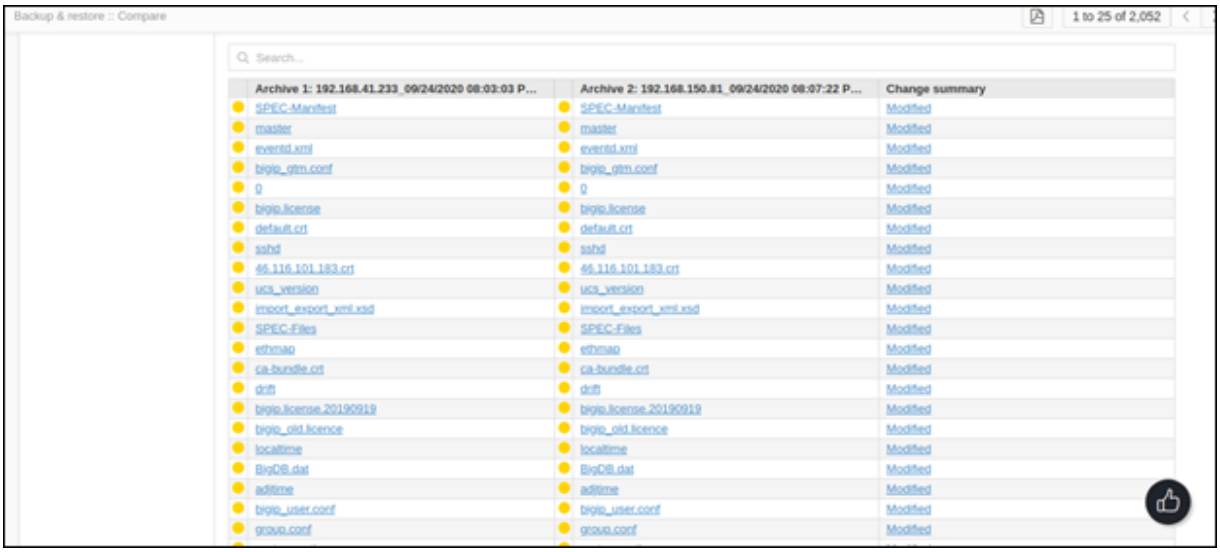
To compare backups for the same or different devices,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Compare Configuration**.
   The **Compare** tab opens.
2. On the **Compare** screen that opens, select the **Compare Type**: Device, Object, or Environment.
3. Select the Device names for which the configuration needs to be compared. The devices that have valid backups generated will be listed here.
4. In the **Device name** field, enter the name of the first device whose backup you want to compare.
5. In the **Archive 1** field, select the first backup in the comparison.
6. In the second **Device name** field, enter the name of the second device in the comparison. If you want to compare backups from the same device, enter the same name you entered in Step 4.
7. In the **Archive 2** field, select the second backup in the comparison.
8. Click **Compare**.



9. A table appears at the bottom of the screen, showing all of the files contained in the two backups you selected. The files are compared globally and a change summary is listed,
   - **Yellow** - Denotes the modifications
   - **Green** - Denotes the new additions
   - **Red** - Denotes the deletions

   Note: Click on the **Modified summary** for a line-by-line comparison of a particular file that is labeled as modified. This will help us to which line of the configuration is modified exactly thus helps to troubleshoot changes faster.
10. Click on the File name to get the configuration details.
11. Change the **Archive name** to compare against a different configuration backup.
12. Get the high-level device file summary and it can be exported using the Export as PDF option.

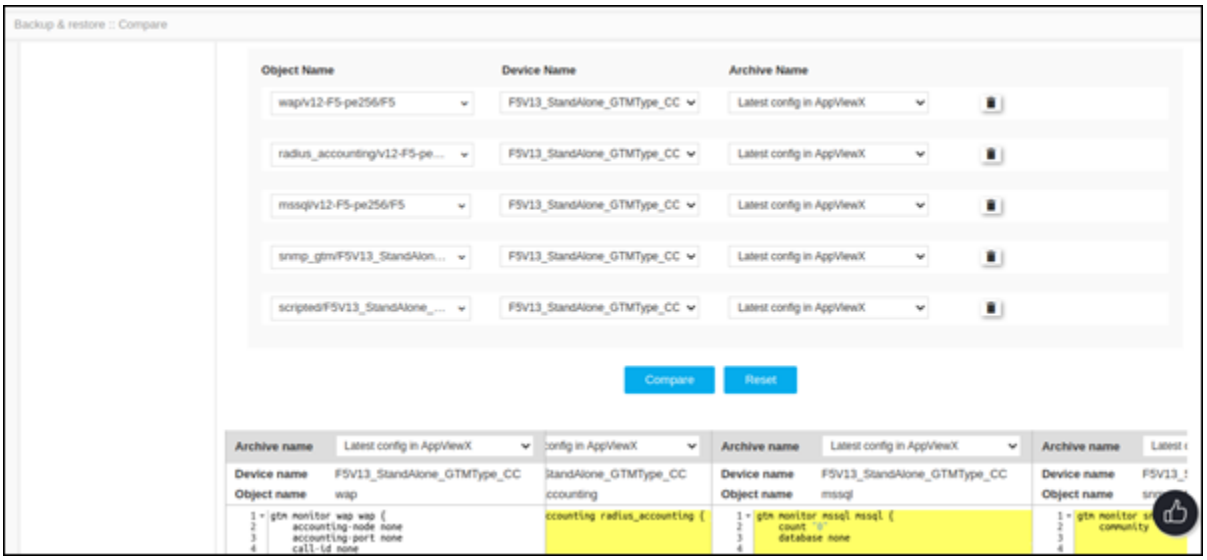


Compare Multiple Configurations of an Object

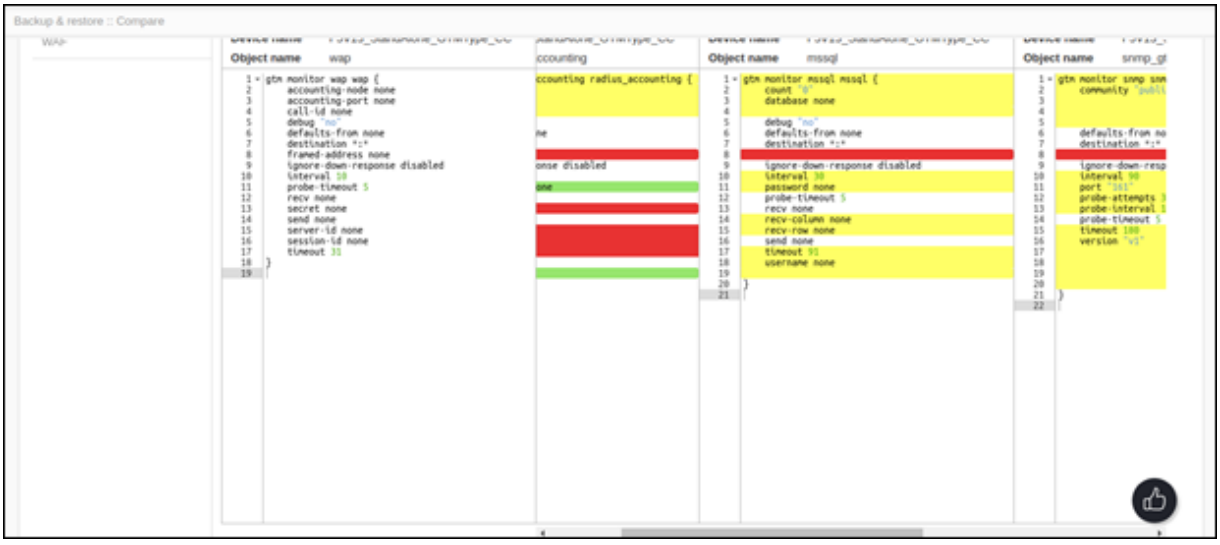
Compare the object-level configuration of load balancer devices using previous backups or the latest configuration in AppViewX. Ensure a particular object (Say iRule) config is compliant across all the devices in a business unit. You can also track the exact configuration changes on your application by comparing them against all the recent archives.

To compare multiple configurations of an object,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Compare Configuration**.
   The **Compare** tab opens.
2. Select the vendor whose objects you want to compare.
3. Select the object type you want to compare. The possible object types are WideIp, GTM Pool, GTM Server, GTM Monitor, GTM iRule, VirtualServer, LTM Pool, LTM Monitor, Profile, LTM iRule, LTM iRule Class, LTM Policy, LTM Persistence, Traffic Record, Traffic Region.
4. Click the **Object Name** dropdown list and select the name of the object whose configurations you want to compare.
5. In the List of Devices field that appears, click the first Device Name dropdown list and select the first device you want to use in the comparison.
6. If you want to compare configurations of the same device over time, choose the device you selected in Step 8.
7. In the **Archive Name** field, select the first configuration you want to use in the comparison.
8. In the second Device Name dropdown list, select the second device you want to use in the comparison.
9. In the second Archive Name field, select the configuration you want to compare the first configuration to.
10. Click the **Add** button to add more configurations of an object.
11. Click **Compare**.



12. The screen refreshes and displays the two archived configurations side-by-side.
13. A maximum of five archives can be compared.

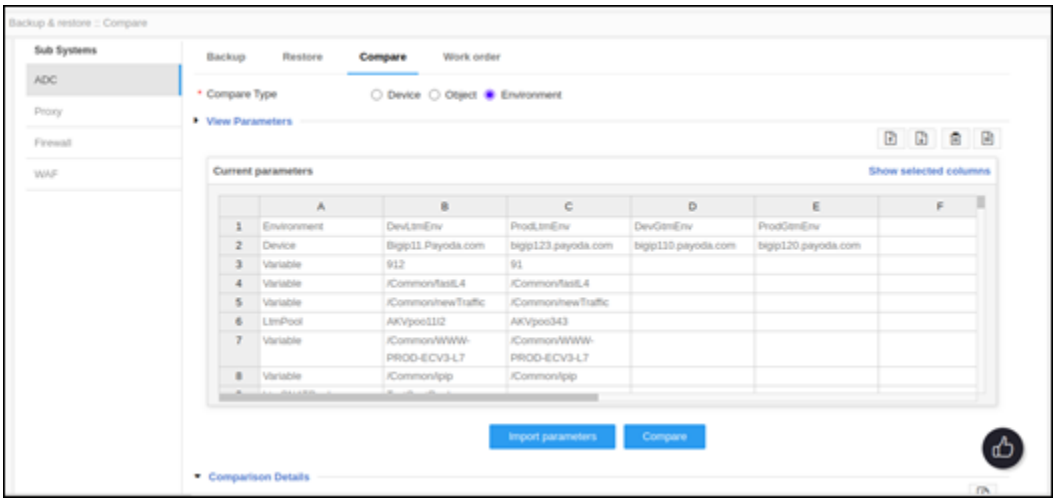


Compare Configurations of Custom Environments

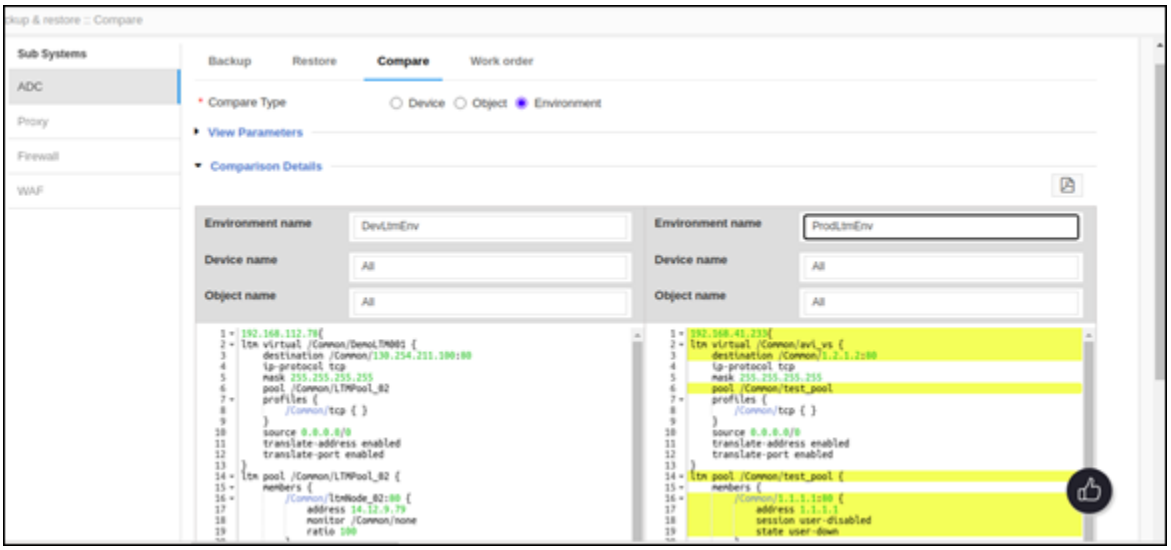
AppViewX allows you to compare the custom environment configuration. A custom environment could be specific to a business unit comprising specific devices and objects. You can import the custom environment details (devices and objects) into AppViewX in the form of an Excel file and compare the source and destination environment configuration of F5.

To compare configurations of custom environments,

1. Click the **Menu** > **ADC+** > **CONFIG MANAGEMENT** > **Compare Configuration**.
   The **Compare** tab opens.
2. In the **Compare Type** field, select the Environment radio button.
3. Click the icon beside **View Parameters** section to expand it.
   The **Current Parameters** table is displayed.
4. In the table, you can export, import, or delete parameters; download the sample using the buttons on the top-left corner. You can also right-click inside the table to delete a row; select, delete or unselect a column.



5. Click **Import Parameters**.
6. Click **Compare** to compare the source and destination environments.
7. Select the environment names, device names, and object names to be compared from the respective dropdown lists in source and destination environments. A line-by-line comparison will be displayed below each environment with the following color coding:
   - **Green** - Denotes the new additions
   - **Yellow** - Denotes the modifications
   - **Red** - Denotes the deletions
8. If required, you can click the (**Export to PDF**) button to download the comparison report to your computer.



Enforce Golden Config Compliance

A “golden” configuration is a configuration version that can be used as a standard configuration for error-free and rapid deployment. Automation workflows help you create golden configurations adhering to organizational policies.

For more details, see the Enforce Golden Config Compliance in the Workflow section.

Chapter 5: AUTOMATION

- Workflow Catalog
- Workflow Request

Workflow Catalog

The AppViewX Platform helps Enterprise IT manage, automate, and orchestrate application delivery services.

Key Advantages:

- Abstract hardware, software, open-source, and cloud solutions from end-users requesting application delivery services
- Orchestrate how GSLB, DNS, load-balancing, firewall, WAF, certificate, network, ITSM, and notification services are leveraged in the multi-cloud infrastructure.
- Integrate industry-leading ITSM and notification services into automation workflows.

- Expose network infrastructure services to DevOps tools like Ansible, Terraform, Chef, and Puppet.
- Build repeatable and compliant infrastructure with workflows that map to your business process.
- Use the business process to enforce how compliance is achieved in multi-cloud data centers.
- Automate how unused resources are returned back to the application delivery infrastructure.

- Enable end-users to self-service and launch automation from application-centric views.

- Enable common load-balancer and DNS service requests to be self-serviced by application and operation teams.
- Minimize the operational expense of maintaining automation workflows when changing vendors or versions.

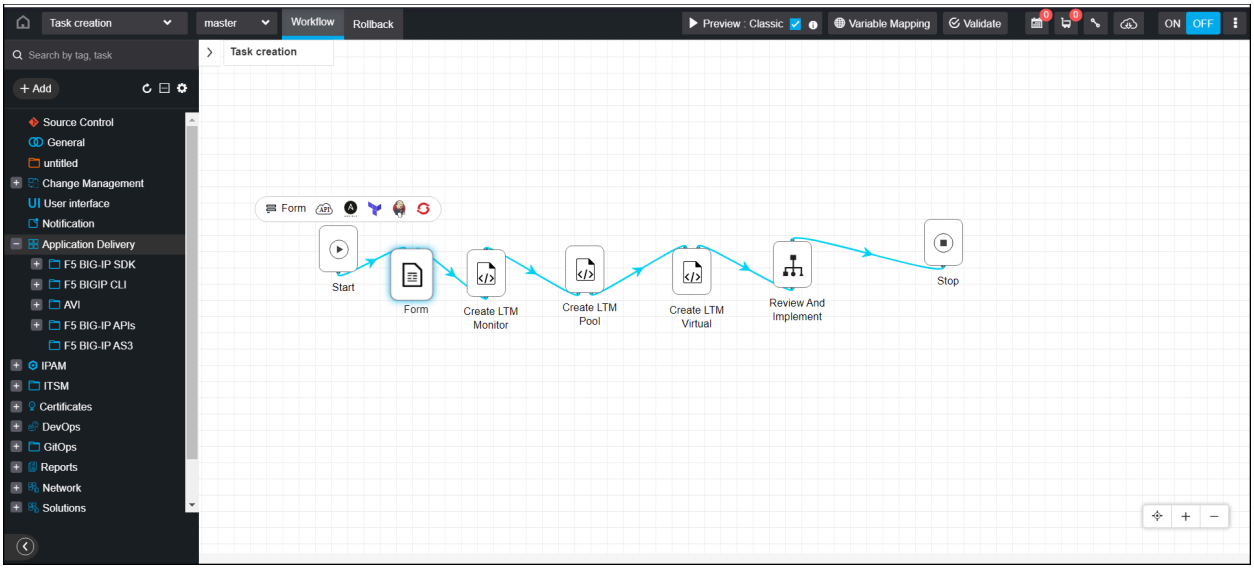
- Automate and Self-Serve ADC deployments with Pre-packaged Workflows
- Orchestrate Changes in App Delivery and Enforce Deployment Standards
- Self-Servicing through Custom Workflows
- Self Service App Catalog

Automate and Self-Serve ADC deployments with Pre-packaged Workflows

AppViewX is a true multi-vendor platform for managing the ever-evolving complex enterprise infrastructure. As your application delivery infrastructure becomes progressively more complex, enterprises must turn to network infrastructure management and automation solutions to ensure successful deployments. AppViewX offers a suite of tools for organizations striving to become true digital enterprises.

The AppViewX platform will help you automate third-party, best-of-breed, and open-source network services like those provided by application delivery controllers, security devices, certificate authorities, DNS servers, routers/switches, and more.

The AppViewX platform integrates with other best-in-class IT service management solutions to govern and record service requests in the larger automated workflow. It can be leveraged to help users move faster, eliminate errors, and reduce costs, making it the best choice for enterprises working to adapt to new technologies, processes, and application delivery expectations.



- Workflow Catalog Page
- Multi-vendor ADC Application Deployment
- Enforce Golden Config Compliance and Migrate Configurations
- Optimize Load Balancer with Unused Object Decommissioning

- Upgrade of Load Balancers
- CVE Reporting

Workflow Catalog Page

AppViewX offers Visibility on the One-touch Automation solution offerings to address network and application service requests. The offerings are available in the Request catalog page. Click **Menu** > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run**. The automation offerings (workflows) are controlled by AppViewX's modern RBAC control feature, thus providing individuals groups to maintain and access their own workflows.

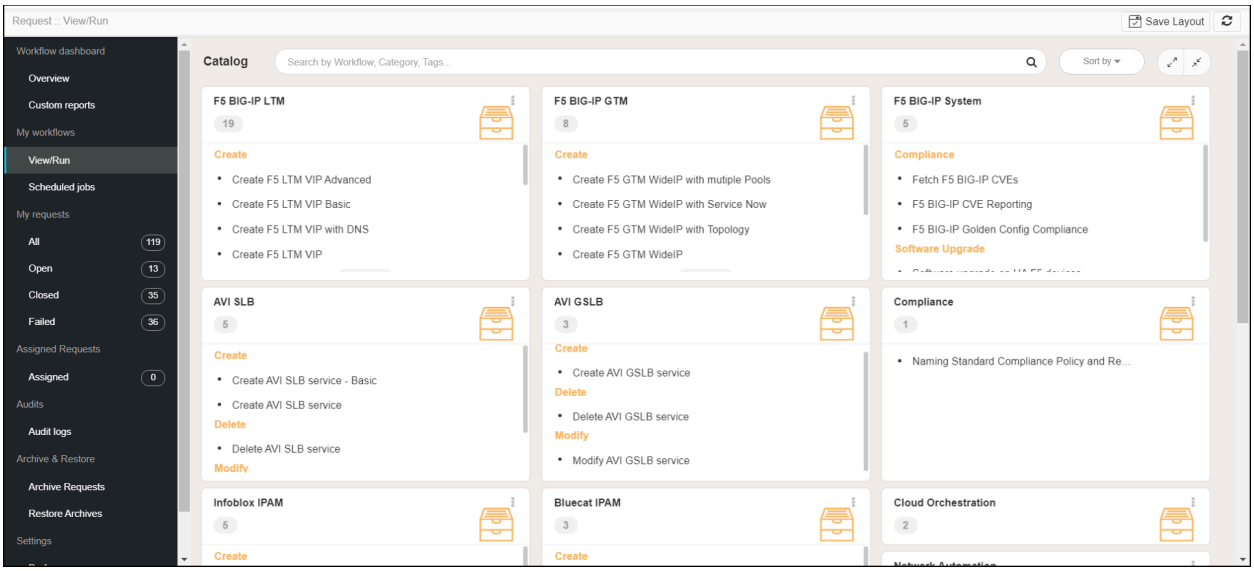
Multi-vendor ADC Application Deployment

As the application deployment in enterprises is complex, time-consuming, and cumbersome, AppViewX's automation solution helps in speeding up the process to bridge the isolation across multiple teams that are involved in application deployment. AppViewX also integrates with leading technology and best-in-class IT service management solutions to govern and record service requests in the larger automated workflow. It can be leveraged to help users move faster, eliminate errors and reduce costs.

The prebuilt automation workflows deliver the following when it comes to Application deployments,

- Creation/Modification/Deletion of WideIPs and Virtual Servers on AppviewX managed ADC devices through simple, self-service forms.
- Integration with DDI (Bluecat, InfoBlox), and ITSM (ServiceNow) enabling a consistent change management control and governance.
- Integration with AS3 (declarative approach) for faster Application deployment by enabling Creation/ Modification/Deletion of BIG IP Application Services.

To access the prepackaged workflows, click **Menu** > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run.** The workflows are grouped as per the vendors, select the required flow and invoke the required flow to deploy/manage an application.



Refer to Visual Workflow Guide for creating workflows

https://pages.appviewx.com/rs/249-TWN-899/images/Guide_App_Provisioning_Automation%20Workflow_AppViewX.pdf.

- Process Flow for Create Virtual Server (sample)

Process Flow for Create Virtual Server (sample)

The Create Virtual Server workflow creates a virtual server and associates it with profiles, monitors, pool, and pool members in F5 LTM using Infoblox and ServiceNow integration. It uses a simple, self-service based approach to gather application-provisioning requirements and generate vendor-specific configurations or REST APIs. This self-service workflow filters F5 ADC devices based on the user's access permissions, defined by Role-Based Access Control (RBAC). The platform integrates with IPAM systems like Infoblox, which allows users to reserve a free IP address from the available address pools and create DNS binding for the new virtual server in Infoblox.

The workflow also includes an option to create or bind existing profiles and monitors to the virtual server and allows users to create change request tickets in ITSM systems ¬like ServiceNow for approvals and tracking. The service request change ID is associated with the work order and is updated based on the implementation status.

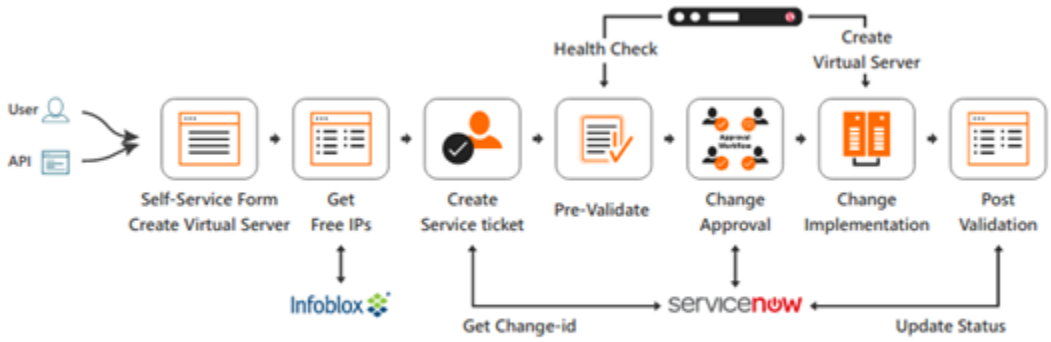


Figure 2: Automate Application Provisioning on ADCs

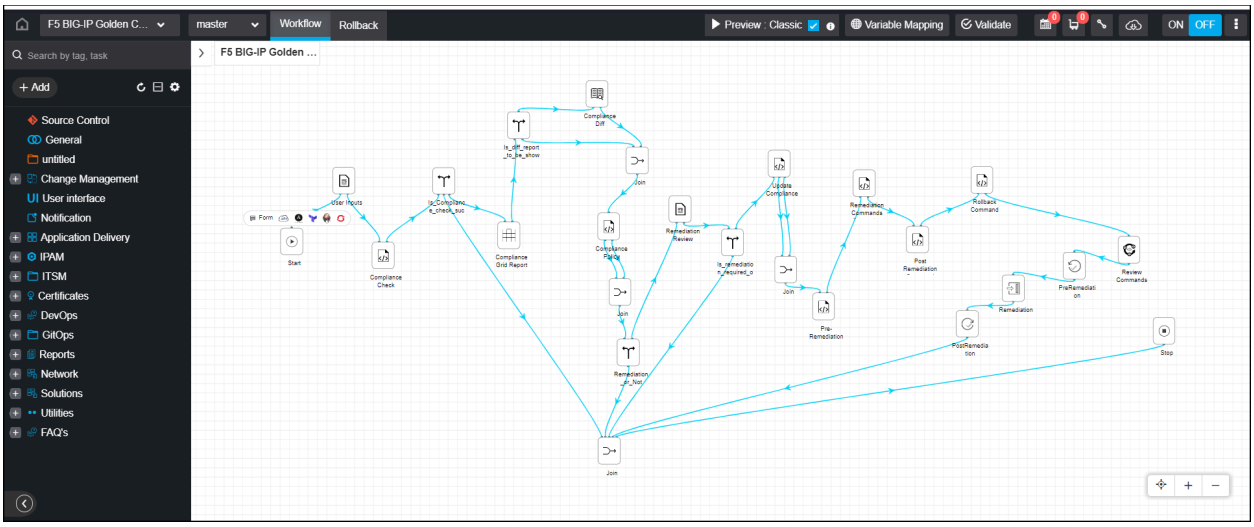
Refer to Automation Guide for more detail.

Enforce Golden Config Compliance and Migrate Configurations

In this digital world, organizations depend on the continuous availability of applications and networks for business success. The advent of digitalization has changed the way the network is being managed. In heterogeneous networks, network leaders face various challenges in properly managing configurations, carrying out changes, ensuring compliance to regulations, and minimizing network downtime triggered by human errors.

AppViewX offers a Prepackaged 'Golden Configuration Compliance on F5 BIG-IP' workflow to run a compliance check across all the managed F5 BIG-IP devices. The workflow is designed to validate the system-wide configurations on F5 Devices for configuration standardization or compliance purposes. Thus maintaining the Integrity and security of an enterprise-level infrastructure.

Click **Menu** > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run** > **F5 BIG-IP System** > **Compliance**. Invoke the workflow 'F5 BIG-IP Golden Config Compliance'.



- Create golden configurations adhering to your organizational policies and store different file variants in the AppViewX collection module.
- Execute the workflow by selecting the Golden configlet file (Choose an existing file or create new) and the devices on which it needs to be applied. AppViewX validates the system-wide configurations on F5 Devices for configuration standardization or compliance purposes.
- AppViewX generates a standard config and pushes it to the end devices based on approvals.

Refer to Automation Guide for more details.

- Compare Configurations in workflows

Compare Configurations in workflows

AppViewX provides a flexible component (Diff checker) to validate the configuration changes over time. As avoiding configuration drift is a major challenge, AppViewX's visual comparison tool that could be integrated into the workflows helps to overcome this scenario and ensures devices are compliant. Access the component by navigating to **Menu** > **Studio** > **Workflow** > **Create** > **Diff checker component.** Drag and Drop the component into the required workflow wherever comparison is needed.

It allows static and dynamic comparison of configurations across two to five devices and objects. Diff View provides a side-by-side comparison of configuration files in a single view. And, it also highlights the configurations that are added, modified, or deleted in different color codes.

With Diff Checker, the AppViewX platform helps to perform compliance configuration checks across devices and allows the configurations to adhere to standards.

- Validate configuration changes between pre-validation and post-validation stages
- Validate for configuration changes between implementation and rollback stages
- Validate for configuration changes between multiple peer reviews within an automation process
- Validate if device configurations are compliant with the standard golden configurations

Optimize Load Balancer with Unused Object Decommissioning

Manage unused configurations during hardware replacement or version upgrades to optimize your load balancers. Set of Virtual Servers/Objects that do not handle traffic for a certain period of time (three months or more) are often referred to as unused objects. Unintentionally maintaining these inactive objects leaves many unwanted IP ports open and their IPs unused and also incur overhead costs for the enterprises. With AppViewX's Application Delivery Automation solution, decommissioning virtual servers can be done in a standardized and automated way.

- Automate the Decommissioning of Virtual Servers

Automate the Decommissioning of Virtual Servers

Invoke AppViewX's Prepackaged workflow solution or customize it accordingly to automate the decommissioning of the virtual IPs identified either individually or in bulk. The unused or free IPs are then moved to IPAM systems.

- AppViewX generates the list of unused objects, Disable and Decommission them automatically based on approvals resulting in,
  - More efficient allocation of IP resources. Unused IPs can be used elsewhere
  - Reduced service costs
  - The elimination of unnecessary management and monitoring overhead

Click **Menu** > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run**. Search for the workflow Get Unused LTM VIP and Delete, Get Unused LTM VIP and Notify, Disable F5 LTM VIP, or Disable and Delete F5 LTM VIP.

Refer to Automation Guide for more Details.

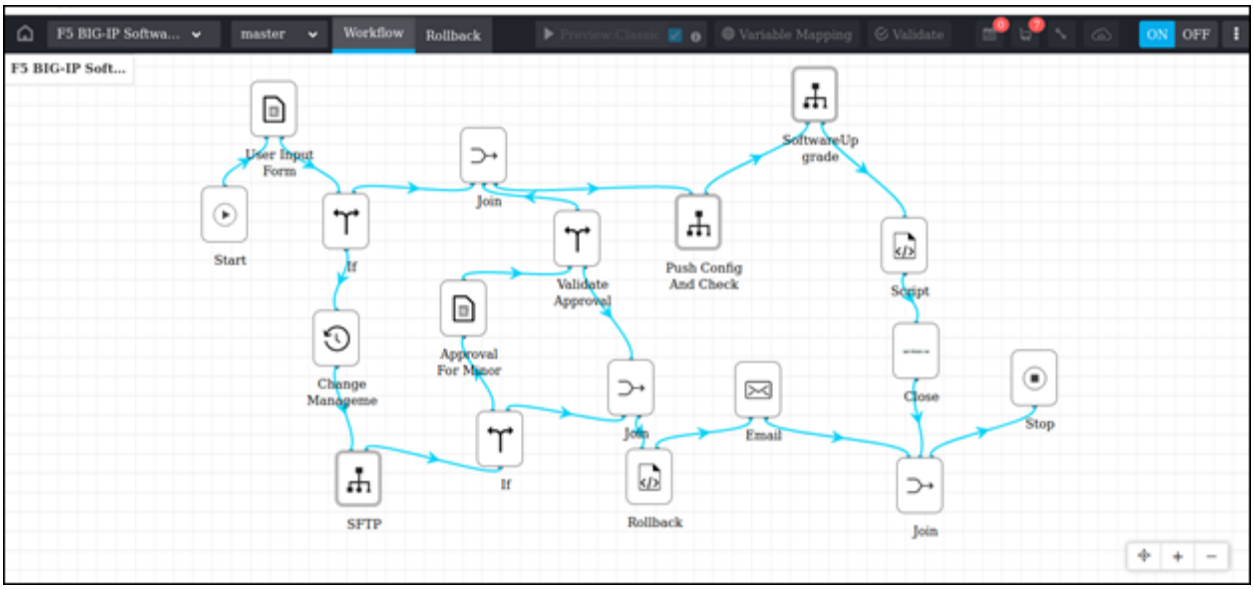
Upgrade of Load Balancers

AppViewX simplifies patch upgrades and version upgrades to the latest F5 version with minimum application downtime. Using AppViewX, you can migrate configurations across different platforms, such as BIG-IP virtual editions and BIG-IP hardware, including the new iSeries platform. Migration through AppViewX ensures clean installation and eliminates errors.

Upgrading F5 BIG-IP devices to their latest versions is a complex, multi-step process involving pre-migration validation checks, UCS back-ups, storing and managing UCS files, updating configurations, and post-migration validation checks. With the phase-out of F5 BIG-IP v10, AppViewX is offering a way to seamlessly transition to F5's latest platforms. By enabling end-to-end automation, organizations can now take advantage of the new features software enhancements can bring, without undergoing a tedious, error-prone migration process.

Click ☰ Menu > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run** > **F5 BIG-IP System** > **System**. Invoke the workflows **Software upgrade on HA BIG-IP devices** or **Software upgrade** on Standalone BIG-IP devices.

The workflow will do necessary Pre checks, Transfer the required software image to the end device, Install the Image, Reboot & Reactivate the license and perform the post validation checks to ensure device configuration is not disturbed. If required, you can customize the steps with a simple drag and drop option and create your own custom flow or add additional approvals.



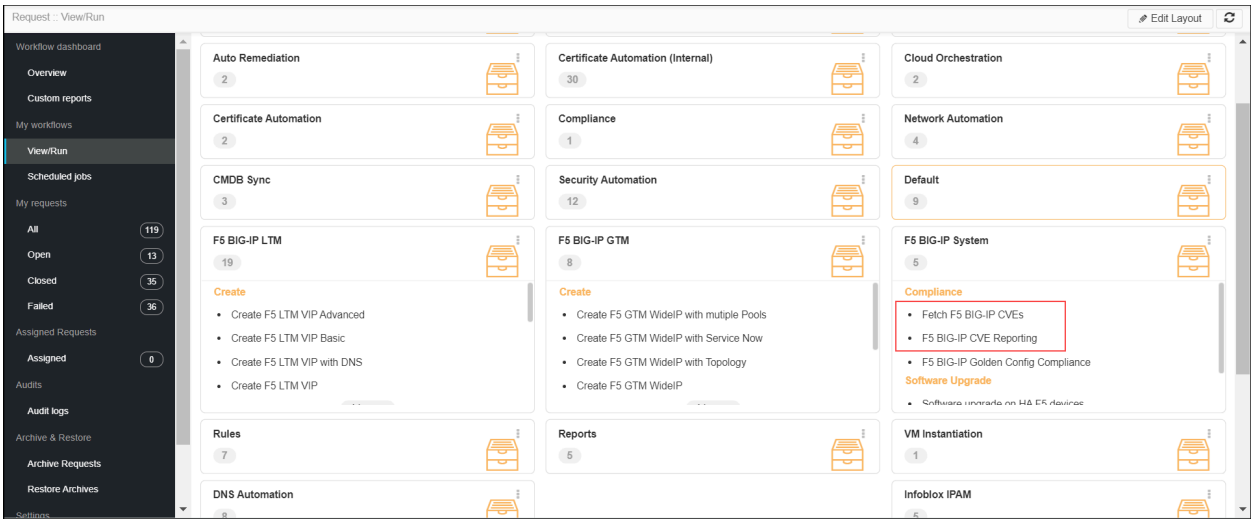
Refer to Automation Guide for more details.

CVE Reporting

The vulnerabilities are informed in the form of reports known as Common Vulnerabilities and Exposures (CVE). At AppViewX, we have designed industry-leading methods where the entire process of validating the CVEs and upgrading an ADC to patch the vulnerabilities is automated from end to end.

You can manage and automate your ADC upgrades with simple task flows which can also be customized as per your requirements. The methods employed by AppViewX are verified, reviewed, and are updated every time we come across something better. Our product allows you to get timely updates from official sources on the latest vulnerabilities that can be obtained whenever you want them. We deliver better than the age-old method of manually checking for vulnerabilities for every single device that you use with just one workflow that brings all that information right to you with ease. To keep track of insecure devices, the discovered vulnerabilities are validated against the ADCs handled in AppViewX, and timely/intuitive reports with severity and suggestions are provided. Post this, upgrades are made to the recommended path version using AppViewX's seamless upgrade flows to resolve the discovered vulnerabilities.

To access the prepackaged workflows, click ☰ **Menu** > **ADC+** > **AUTOMATION** > **Workflow Catalog** > **View/Run.** The workflows are grouped as per the vendors, select the required flow and invoke the required flow to deploy/manage an application.



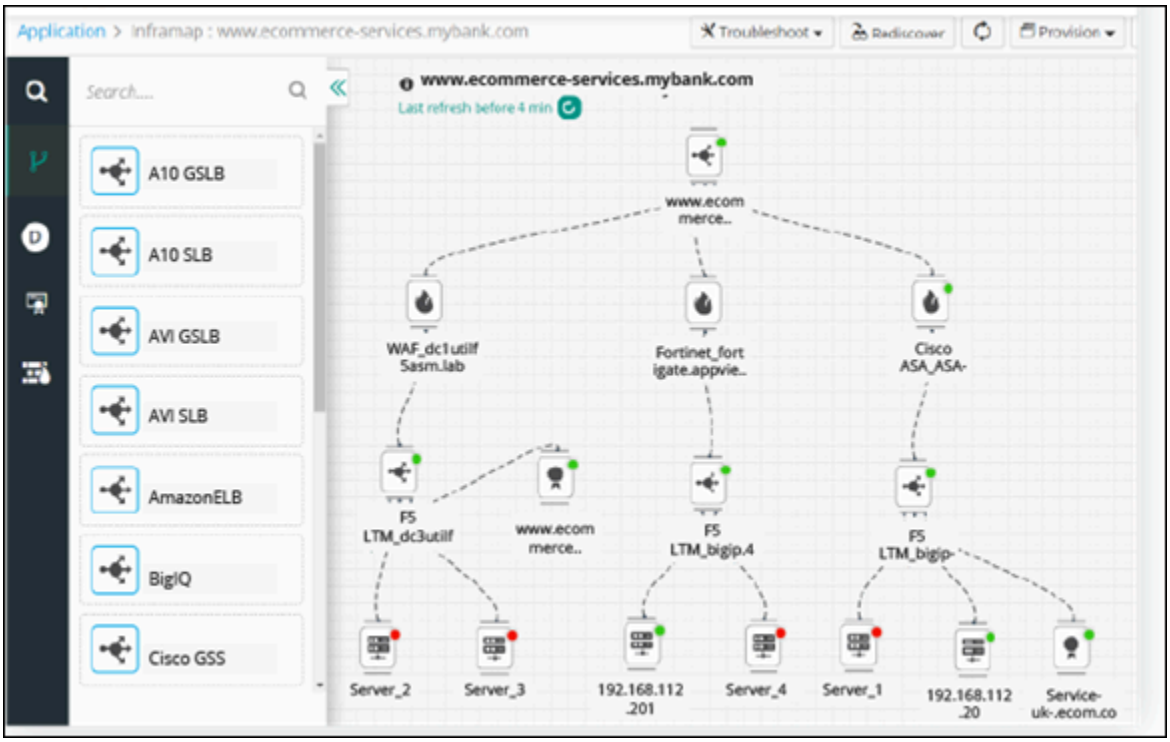
Orchestrate Changes in App Delivery and Enforce Deployment Standards

- Orchestrate Application Delivery in Multi-Cloud Environments
- Orchestrate Application Delivery with DevOps Integration Tools
- Connecting AppViewX with Ansible
- Orchestrate with Ansible Integration

Orchestrate Application Delivery in Multi-Cloud Environments

AppViewX accurately abstracts hardware, software, open-source, and cloud solutions from end-users requesting application delivery services and can be used by business processes to enforce how compliance is achieved in multi-cloud data centers. It can be efficiently used to orchestrate how GSLB, DNS, load-balancing, firewall, WAF, certificate, network, ITSM, and notification services are leveraged in the multi-cloud infrastructure. Through the pre-packaged solutions, enforce deployment standards defined by an organization and orchestrate changes without compromising on security.

Build your own end-to-end orchestration services through the pre-defined solution components available in the Workflow module. Click **Menu > Studio > Workflow > Create Flow.** Drag and drop the components as needed to build your own service.



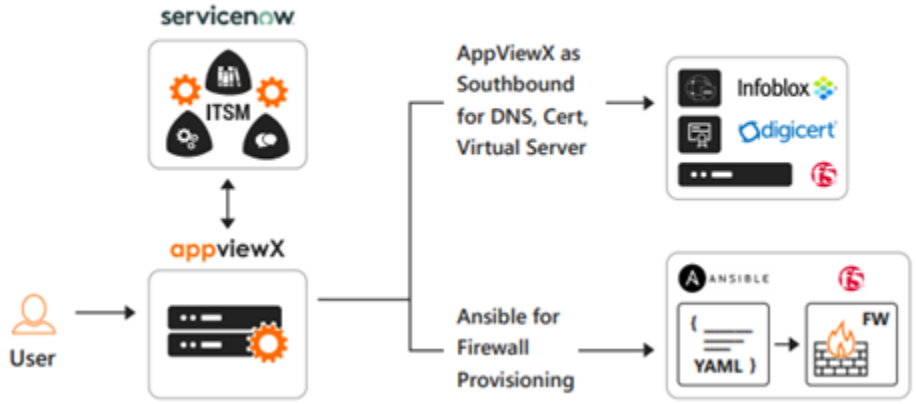
Refer to Automation Guide for more detail.

Orchestrate Application Delivery with DevOps Integration Tools

AppViewX exposes the network infrastructure services to DevOps tools like Ansible, Terraform, Chef, and Puppet. It integrates with the tools to build repeatable and compliant infrastructure with workflows that map to your business process. Enable end-users to self-service and launch automation from application-centric views and Automate the ticketing and governance of DevOps service requests with ITSM tools.

Advantages of using DevOps tools with AppViewX:

- Highly scalable and adaptive
- Zero learning curve
- Define once, deploy everywhere
- DevSecOps-friendly
- Application-centric visibility
- Context-aware troubleshooting and auto-remediation
- Centralized management and extensive integrations
- Comprehensive network and application security management



For more information, click here.

Connecting AppViewX with Ansible

AppViewX can be run on the same control node where Ansible is installed. AppViewX can function as both Northbound and Southbound for Ansible.

AppViewX as the automation controller; Ansible as Southbound:

- You can import Ansible playbooks into AppViewX and call the appropriate ones to construct workflows in the Visual Workflow builder. You can also view and edit the playbook contents from inside AppViewX.

Examples:

- Application provisioning across F5 BIG-IP LTM, AFM using Ansible playbook.
- Instantiate a new server on AWS using AppViewX and Ansible

AppViewX as the orchestration controller; Ansible as Northbound:

- You can download an Ansible module file and a sample YAML file for the required AppViewX workflow on demand. Upload the Ansible module files onto the Ansible Server, provide input using the sample YAML file and execute the module file (playbook) on the Ansible server.

Examples:

- Application provisioning across F5 BIG-IP LTM, AFM
- Automating server instantiation and pool member addition using Ansible

Refer to Automation Guide for more detail.

Orchestrate with Ansible Integration

AppViewX integration with Ansible playbooks makes end-to-end network automation more intuitive, flexible, and user-driven.

- Integrated automation approach to aligning and achieving business goals
- Implement automation with AppViewX and Ansible for continuous delivery

Ansible - Ansible can be used to automate specific instances in the network, like configuring switches ad-hoc and opening firewall ports. Ansible's CLI-based automation has the capability to drill deep into the network, and since it's agentless, can be used on any device from any vendor.

AppViewX - AppViewX is an end-to-end low-code network orchestration and security solution. It handles high-level network operations like real-time monitoring and reporting, key/certificate provisioning and management, context-aware troubleshooting and auto-remediation, and self-servicing capabilities. While Ansible (Core) is CLI-based, AppViewX is GUI-based. It uses REST API to connect with third-party tools and cloud platforms

Self-Servicing through Custom Workflows

Increase the operational efficiencies of your organizations by enabling self-servicing through AppViewX's custom workflow capabilities. The workflow-centric automation leverages various components of the network infrastructure and helps in defining a logical flow of activities or tasks needed to deliver a service from start to finish.

The workflow studio is a repository that contains all the pre-packaged and custom workflow solutions. Manage your workflows from this studio and Create, Delete, Edit, Enable, Disable, or Clone the workflows as needed.

- Design Custom Workflows

Design Custom Workflows

Automate your network infrastructure business process and enable Self Servicing for Application teams through the creation of custom workflows.

AppViewX's Visual Workflow tool provides an intuitive system for designing self-serviceable, event-driven, intelligent, and automation workflows. It enables operational agility and service efficiency in the various

stages of network and application service delivery. It helps to accelerate time-to-value by providing everything needed for the complete automation of application delivery network infrastructure.

Click **Menu > Studio > Workflow**. Start to design your custom workflows. Following are some of the capabilities available in the workflow studio.

- Design workflows using the library of tasks supporting multi-vendor ecosystem on F5, AVI, A10, Citrix - Solutions, and Libraries
- Intelligent work order execution - execute tasks sequentially or in parallel
- Build custom Email tasks in each stage with required parameters
- Validate configuration changes using Pre and Post validation checks
- Configure Reviews/Approvals at each stage to execute a change
- Plug and Play integrations into ITSM systems - Service NOW, Jira, etc.,
- Plug and Play integrations into DDI systems - Infoblox, Bluecat, QIP, etc.,
- Design Rollback workflows in case of execution failure or on a need basis.

Key Advantage:

- Build custom, event-driven automation using pre-built tasks and workflows
- Integrate with ITSM tools for ticketing and governance or send an email and Slack messages
- Expose a catalog of service requests for network security management
- Enable self-service to automation workflows with user-friendly forms

Self Service App Catalog

AppViewX provides a one-stop portal with all the service offerings in the form of low code pages to enable self-servicing for the end-users (like App owners, Network Engineers, CA, Admin, etc.) in a simplified and intuitive manner. There are Out of the Box catalogs and as well option to customize catalogs as per the organization standards. Access the opinion through **Menu** > **Studio** > **Pages**.

Benefits

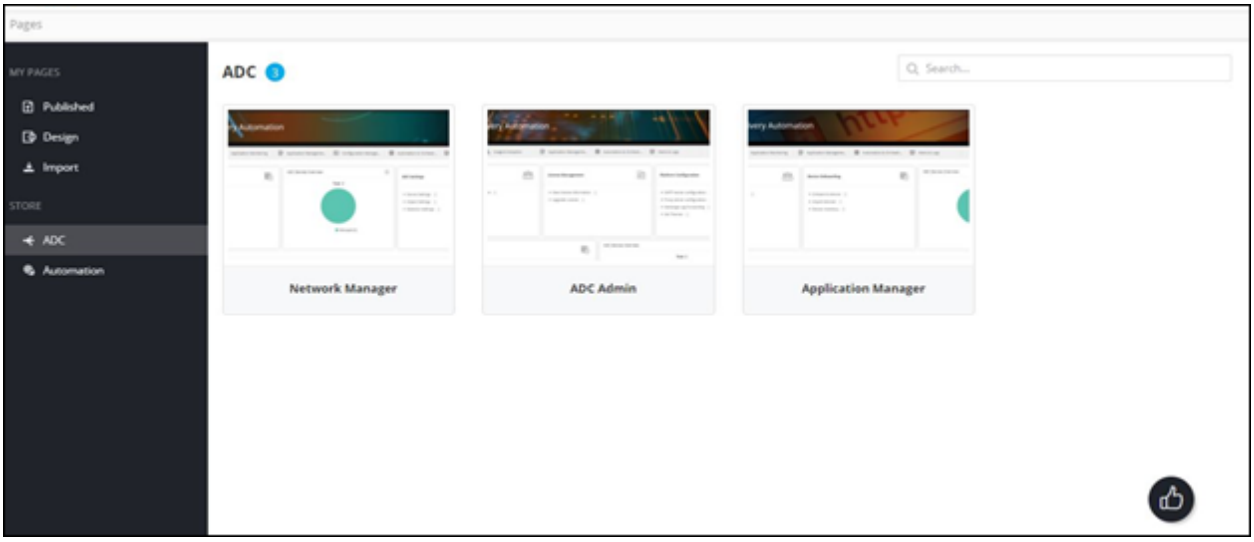
- An intuitive self-service portal to access all service offerings for employees, and partners via Single Pane of Glass.
- Customer Experience – Users only see services that are available to them, described in business terms they understand.
- Build your own App catalog/portal.

- Configurable Catalog page that allows for personalized task views.
- Low Code designer portal – Low Code and configurable toolsets, allowing users to brand Catalog solution so it feels familiar and intuitive for the end-users.

Self Service Catalog for ADC Roles

AppViewX provides out of the box self-service catalog page for the ADC Roles based on the permissions assigned. Refer **Roles**for more details about the out of the box roles.

Access the catalog through, **Menu** > **Studio** > **Pages** > **ADC store**.



The catalogs comprise all following relevant functions and the life cycle of Application delivery presented in the form of a journey thus enabling a seamless self-servicing experience to the end-users. The catalogs could be cloned to achieve any sort of customization.

- Discover/Onboard
  - Discover Devices
  - Onboard users and control access
- Application Visibility – Control Center engine
- Monitor - Application delivery reporting

  - Health Reports
  - Performance Reports
  - Drift and Alerts
- Application Management and Monitoring
  - Build Application View/Traffic Failover Widgets
  - Build Live Traffic Monitoring Widgets
  - Build Application Dashboards
- Automation and Self-servicing workflows
- Configuration management
- Application, Device Alerts, and Remediation

Design Your Own App Catalog

On clicking design, you will have options to design a custom app catalog. Define a name and description for the catalog. Drag and Drop some of the following components to build a catalog,

- Custom Branding
- Drag and Drop Reports/Workflows
- Enable Quick links to the solutions
- Configure External links
- Embed Page/Logo/Widget
- Design custom section using HTML editor palette
- Tab menu component for Horizontal, Vertical tab menus

Publish and Share the Catalogs to End-users

Assign/Share the custom catalog page/workspace to specific user groups, users. The users with the shared pages can start accessing the functions available in the pages based on their RBAC.

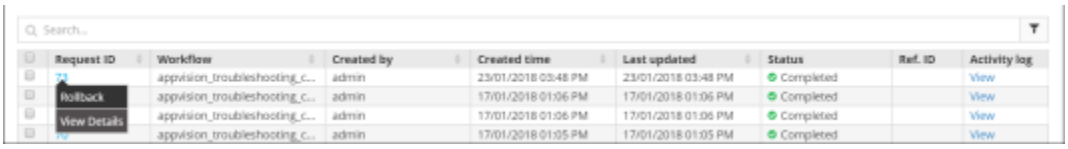
The catalog page could also be set as a landing/home page to enable a simplified journey to your end-users.

Refer to Pages Guide for more detail.

Workflow Request

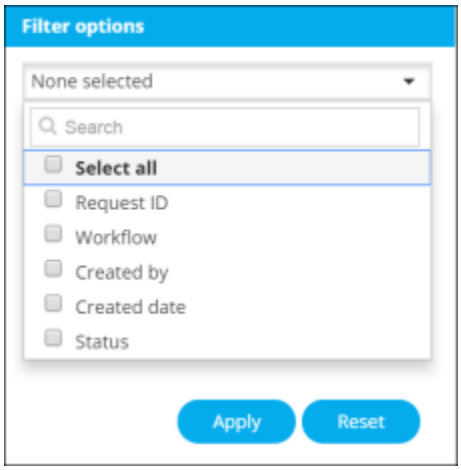
You can group your workflows accordingly and create a workflow catalog. The list of grouped workflows in the catalog will be displayed in this section.

- The **Workflow Request** section displays the total number of **All**, **Open**, **Closed**, and **Failed** requests, clicking upon these tabs displays the corresponding workflow details in a table.
- You can also perform the following tasks:
  - Right-click the **Request ID** and select one of the following options from the pop up that appears:
    - **Rollback** - Triggers an alternative rollback workflow that you have added or imported for the workflow.
    - **View details** - Displays all the tooltips configured in the Global variables.



  - From the **Request ID** column, you can click on the request for which you want to view the details. On the tabs in this screen, you can perform the following tasks:

    For the workflow(s) containing grid component(s) and script(s) to generate data, you can click the (**Download**) button to save the data to PC in XLS or CSV file format.
  - Search for a request using the **Search** field.
  - Click the (**Filter**) button to select the options you want to use to sort the requests.



Chapter 6: ALERTS & LOGS

Alert

Alerts Overview

Alerts are a construct intended to inform administrators of significant events or complications that occur within the application. AppViewX provisions Proactive Application Service Monitoring & Alerting for quick remediation.

Alerts could be raised based on various metrics. In AppViewX, alerts are Device and Application based and each has its severity level. Severity levels are as follows:

- Critical
- Fatal
- Major
- Minor

AppViewX receives alerts only for devices that have been subscribed to AppViewX.

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.

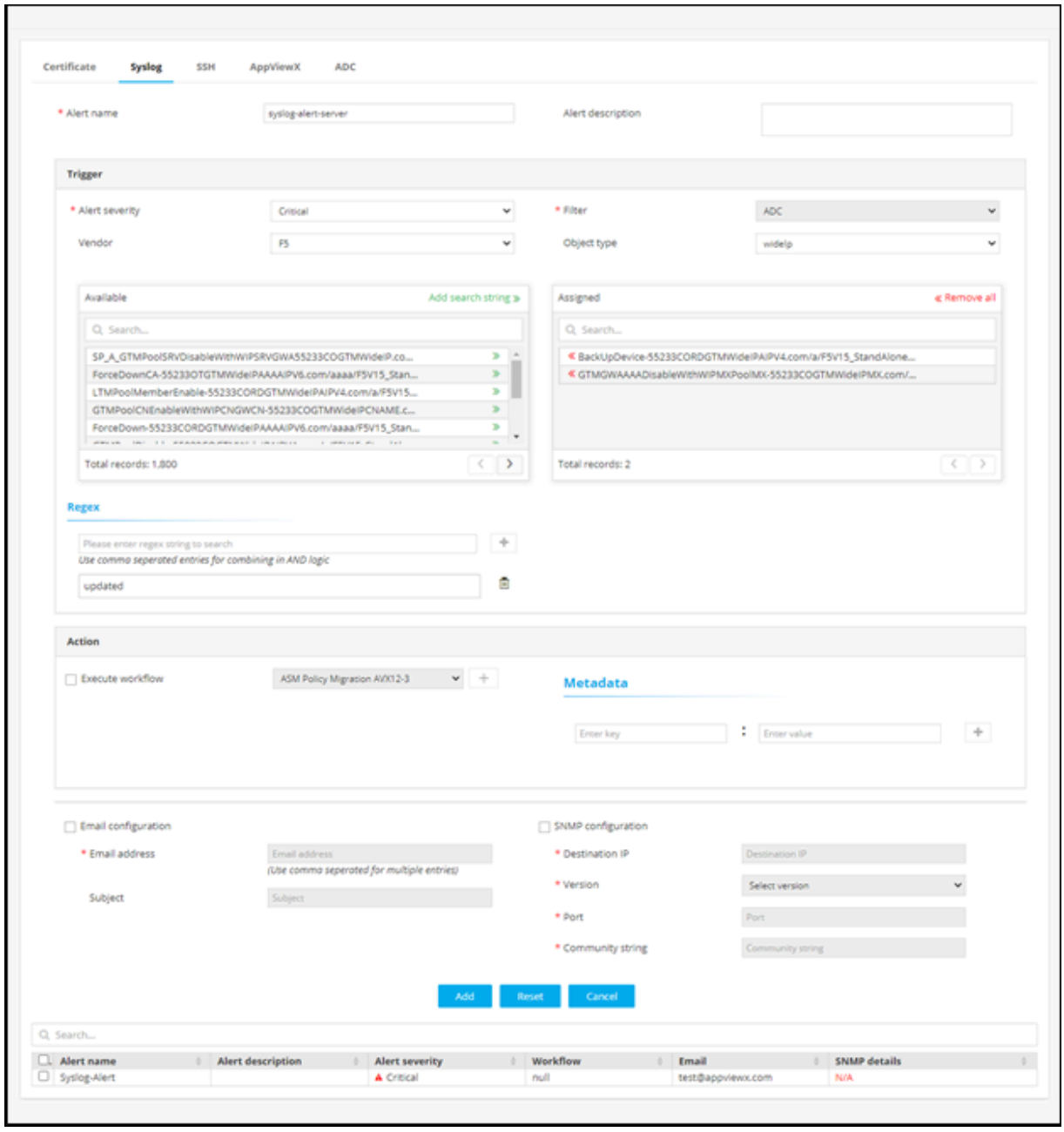
Create a Syslog Alert

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.

Email/SNMP Alert Notifications

AppViewX supports notifications via Email and SNMP based on the configuration to improve the chances of remedial action.

To get notified via Email, **SMTP** must be configured. To configure For SMTP configuration, refer to Platform User Guide. You can provide multiple Email addresses with Subject lines to receive the alert.

To get notified via SNMP (Simple Network Management Protocol), following information are required:

- Destination IP and Port
- SNMP version (v1 or v2)
- Community String - The string is similar to a user ID or password

AppViewX Alerts

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.

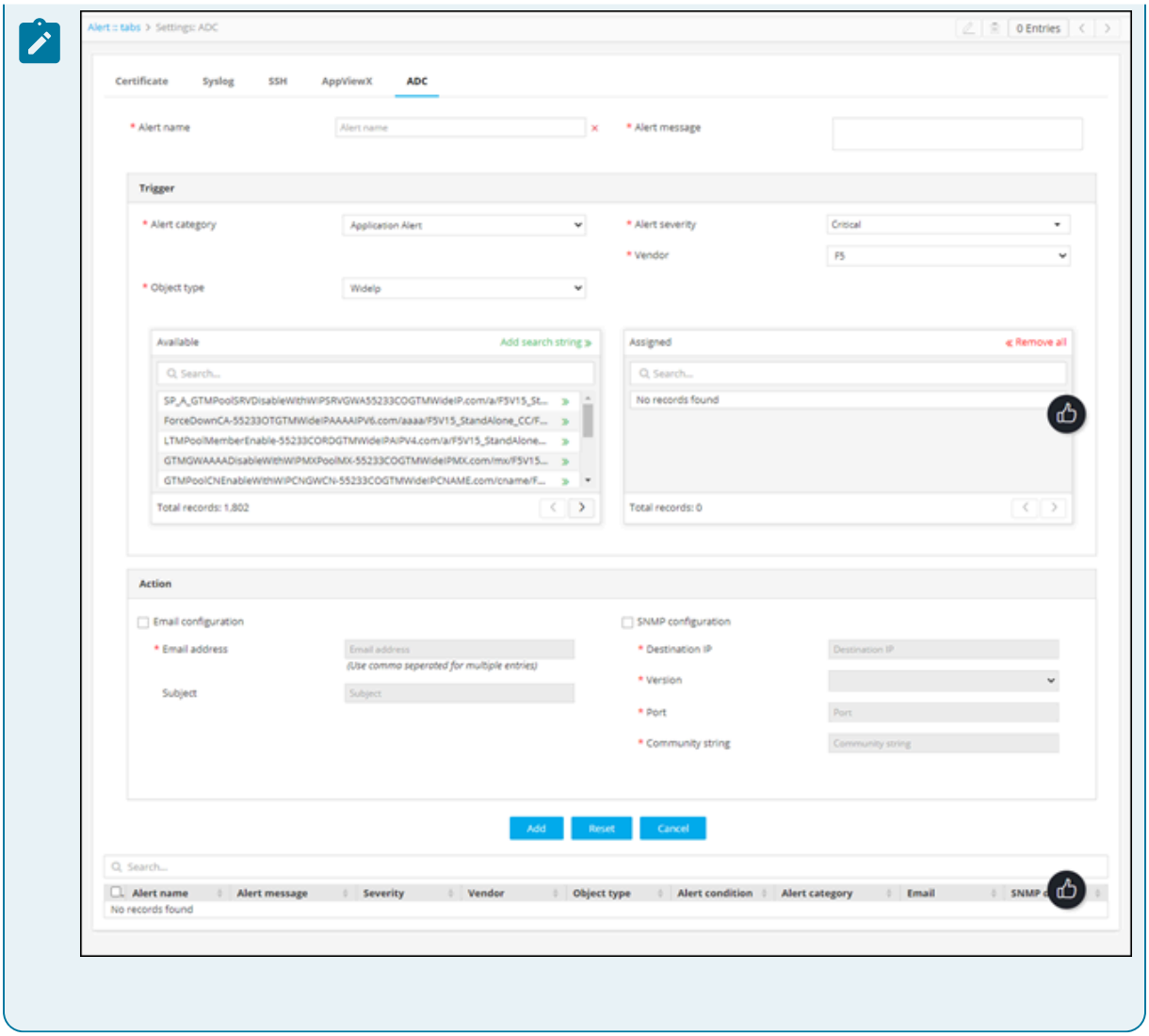
To configure Syslog alerts,

1. Go to **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts**.
2. Click (**Settings**) icon, and then ADC.
3. Enter an Alert name and Alert message.
4. Select the **Alert Category** from the drop-down list. The options are **Application Alert** and **Device Alert**.
5. Select the **Alert Severity** from the drop-down list.
6. Configure the critical **Device/Applications** that need to be monitored.

Note:

Note:

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



7. 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.
8. 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 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.
- 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.

Threshold Alert

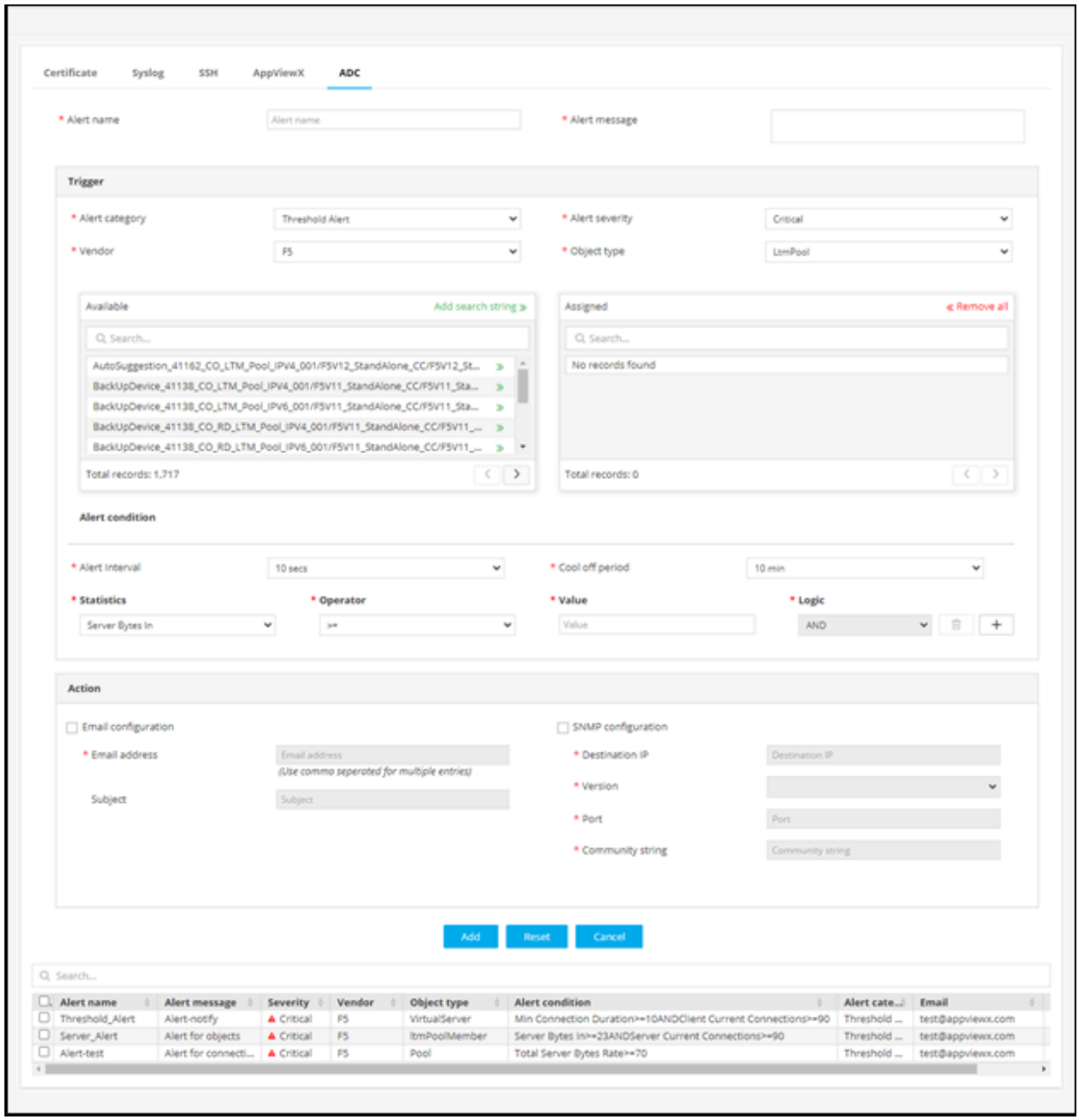
AppViewX allows near real-time monitoring of Critical Applications/Devices that breaches statistical thresholds like CPU, Memory, Number of requests, etc. Customize the threshold limits as per your organization, monitor Apps on real-time, and get notified via Email or SNMP.

To configure Threshold Alert,

1. Go to **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts**.
2. Click (**Settings**) icon, and then ADC.
3. Enter an **Alert Name**, **Message**, and **Category** as Threshold.
4. Configure the critical Devices/Applications that need to be monitored.
5. Set an Alert monitoring interval from 10 secs to 60 secs that fetches the run time data from the device to validate against the threshold.
6. Set a Cool off period like 10, 20, or 30 mins. The cool-off period prevents the user from getting bombarded with notification alerts for the same event.
7. Configure the Statistics that need to be monitored and set a value ie >=,<=,<,>,==.
8. Create an Alert with multiple conditions with Logic AND and OR by clicking .
9. Define a Severity for your event based on the threshold conditions (Critical, Fatal, Major or Minor).
10. Configure the notification type as Email or SNMP.
11. Configure multiple Alerts as needed and Add them to the Grid. The configured Alerts could be modified or deleted anytime by selecting the Alert from the grid.
12. Following are some of the alerts that can be configured:

- A Virtual server’s Current connection exceeded 100
- A critical Device’s CPU breaches 60
- A server’s Number of Requests is lesser than expected.

13. The configured events will be notified to the end user via Email or SNMP and as well captured in the Alerts inventory for tracking.

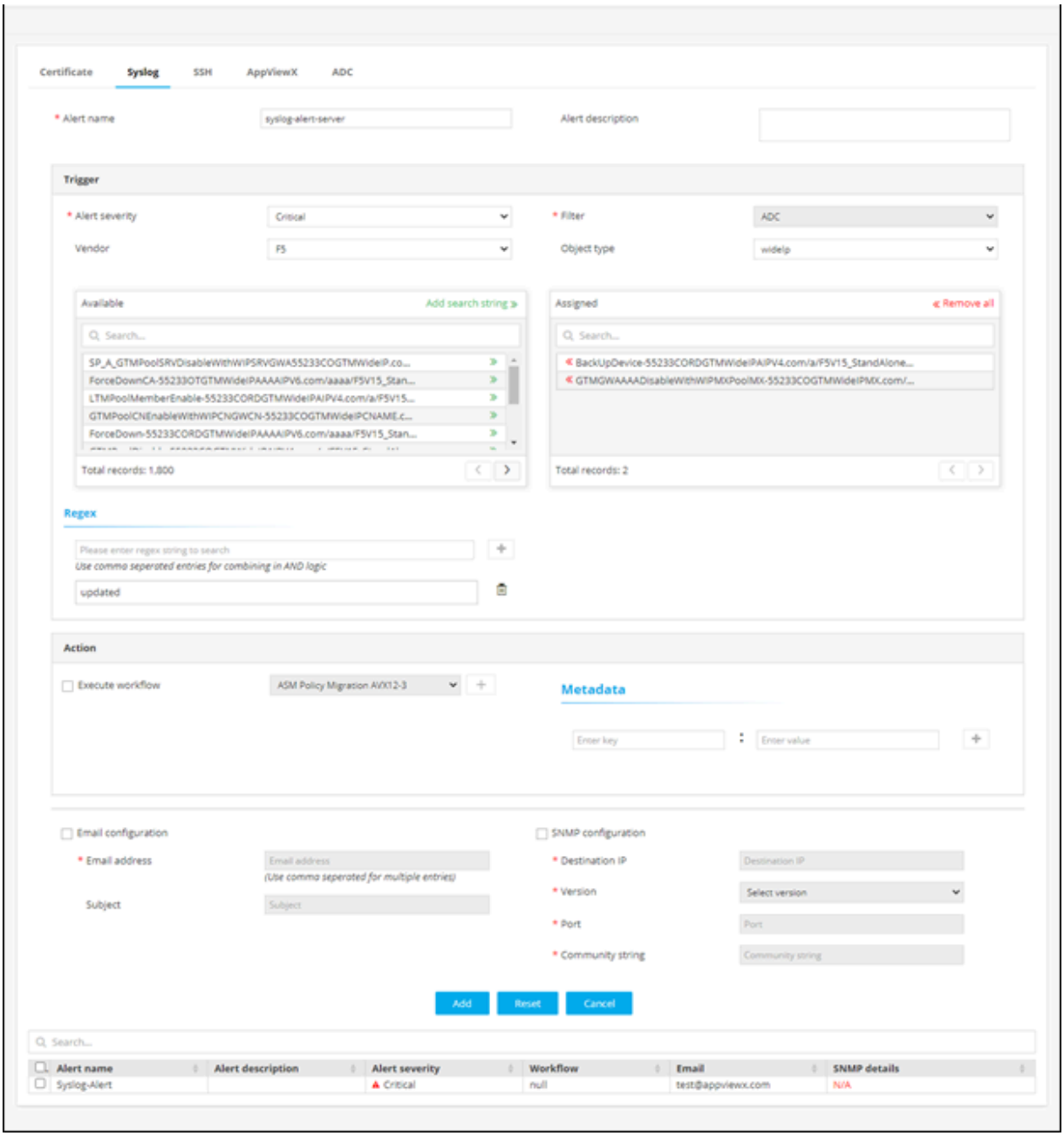


Monitor Critical Applications/Devices and Receive Notification

Alert settings can be configured to trigger Email/SNMP alerts when any action is executed on configured Application(s) or Device(s).

To configure Application/Device alerts,

1. Go to **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts**.
2. Click (**Settings**) icon, and then ADC.
3. Enter an **Alert name** and **Alert message**.
4. Select the **Alert Category** from the drop-down list. The options are **Application Alert** and **Device Alert**.
5. Select the **Alert Severity** from the drop-down list.
6. Configure the critical Devices/Applications that need to be monitored.



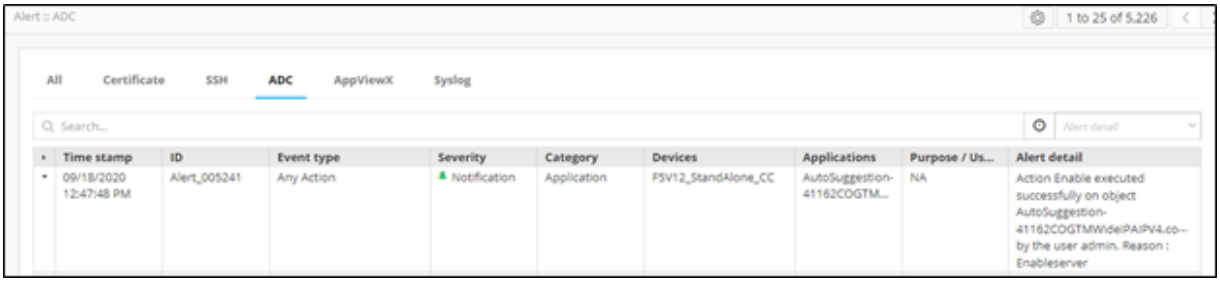
7. In the **Action** section, select the checkbox of Email or SNMP.
8. (Optional) Configure multiple Alerts as needed and Add it to the Grid. The configured Alerts can be modified or deleted anytime by selecting the Alert from the grid.
9. Following are some of the alerts that are notified upon configuration:
   - A critical Application is Disabled or Forced down (Event - Any Action)
   - A critical Device is Restored to a different configuration (Event - Restore)

- Device Flipped from Active to Standby (Event - State change)
- A critical Device is Failed during a config fetch (Event - Status change)
- Device Backup failed (Event - Backup)

Application/Device Alert

ADC specific Application/Device actions executed from AppViewX (Control Center or Dashboards) will be raised as an alert captured in the alerts inventory.

1. Navigate to ADC alerts inventory by clicking **Menu** > **ADC+** > **ALERTS & LOGS** > **Alerts** > **ADC** tab.
2. All the successful and failure events are captured in the alerts inventory along with the user comments. This enabled an Admin to track end-user actions.
3. Every alert contains the following information:
   - Alert ID
   - Alert Event type
   - Severity
   - Category
   - Devices
   - Applications
   - Alert Detail
4. Search for any alert by the Application, Device name or message etc.,
5. All Successful actions are tagged as Notification and Failure as Critical alerts respectively.
6. Event type helps to identify the type of event - An action event or Restore event or Backup event etc.,
7. An example of Object Enable Alert:



8. An example of Device status change alert (Managed to Unmananged):

Logs

- Logs Overview
- View Details of a Log
- Schedule Log Reports
- Forward a Log

Logs Overview

Logs keep track of all activities that take place within AppViewX or any external entity that is connected to the AppViewX system. The Logging functionality in AppViewX tracks user activities and creates the device and object-level event logs.

The Logging screen allows you to view logs, which are grouped into the following categories:

- **All** - All category logs are displayed in this section. The logs listed are based on the latest user actions.
- **Audit** - All user-related changes
- **Self-audit** - Logged in user changes
- **ADC** - ADC specific logs
- **AppViewX** - AppViewX infrastructure level logs
- **Syslog** - End device level logs

Syslogs

- AppViewX subscribes to all device-level logs, where it acts as a Syslog listener. Appviewx registers for Syslog notifications with the devices managed in AppViewX or with external servers (like Kafka) and receives notifications when a change is identified on the device. Based on the notifications, the

AppViewX system shall automatically update the configurations based on a configured interval ensuring device changes are up-to-date.

- Syslogs received from the devices and the changes that are processed in AppViewX based on the Syslogs will be captured in the logging module.
- Following are the events handled by AppViewX:
  - Syslog-based updates for Object state change eg: Enabled, Disabled, etc.,
  - Syslog-based updates for Object status change eg: Available, Offline, etc.,
  - Syslog-based updates for Device failover state eg: Active, Standby, etc.,
  - Syslog-based updates for Creation/Modification/Deletion of Primary objects eg: WideIP, Virtual Server, etc., and Secondary objects eg: Monitor, Profile, etc., at an interval of 15 mins.
    - When there are configuration updates on the objects like a new member added/removed/modified, it will be automatically reflected in the AppViewX database with respective object mapping.
    - If those hierarchy objects are configured in ACL/Dashboard, the permission and actions will be automatically assigned respectively.
- Refer to Installation & Upgrade Guide for more details and Syslog configuration in AppViewX.
- AppViewX can either handle logs directly from the device (Lostash IP registration directly on the device) or through external servers. If the user has enabled Kafka properties, the Logstash registration will be automatically removed from the device.
- AppViewX integrates with external log servers like KAFKA when the Syslogs are not allowed to be received from load balancers directly.
- Kafka is a cluster that runs on one or more servers used to store real-time logs for a device. Ensure that the external log server details are configured in AppViewX to fetch the device logs.
- Refer to Platform User Guide for more details and Kafka configuration in AppViewX.

Within the Logging screen, you can perform any of the following actions:

- View details of a log
- Configure logging for ADC object types
- Export logs

View Details of a Log

To view log details,

1. Navigate to **Menu** > **Logging**.
   The **Logging** screen opens.
2. All the logs are displayed by default.
3. Click the tab that corresponds to the type of log you want to view.
4. On the log screen, view all details for a log by hovering your cursor over each column of data or click the ▸ (**Expand**) icon for the log you want to view. The table row expands to display all details for the log.

> **Note:** Search for any logs from the logging list based on User, Device name, log message, object details, source IP, AppViewX node, Method of login also search based on a particular column.

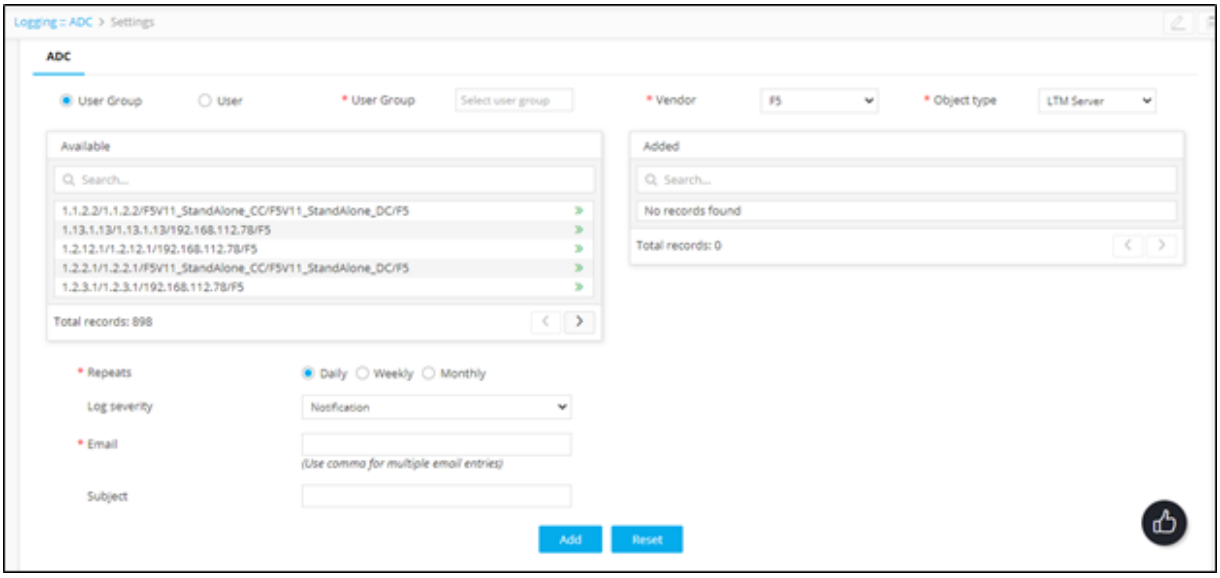
Schedule Log Reports

In addition to providing scheduled logging activities, AppViewX allows you to set up logging tasks for specific ADC object types and have the log results emailed automatically to designated recipients.

1. Navigate to ☰ **Menu** > **ADC+** > **ALERTS & LOGS** > **Logs**.
   The **Logging** screen opens.
2. Click the  (**Settings**) button on the top.
3. At the top of the **Settings** screen, select the User Group or User radio button and then enter the name of the user or group that the log report relates to.
4. In the **Vendor** field, select the vendor whose object or objects you want to generate a log report for.
   In the **Object Type** field, select the object that you want to generate a log report for.
5. In the **Available** field, click the » (Assign item) icon beside each object you want to include in the log report.
6. In the **Repeats** field, select how often you want the log report to be generated: Daily, Weekly, or Monthly.
   From the **Log severity** dropdown list, select one of the following:
   - Critical
   - Fatal
   - Major

- Minor
- Notification

7. This is to let the user know the severity of the log reports that have been sent.
8. In the **Email** field, enter the email addresses of users receiving the log report.
9. (Recommended) In the **Subject** field, enter a short, clear description of the log report so that the email recipients can tell at a glance what the message contains.
10. Click **Add** to add the log report generation task to the table at the bottom of the screen.



Forward a Log

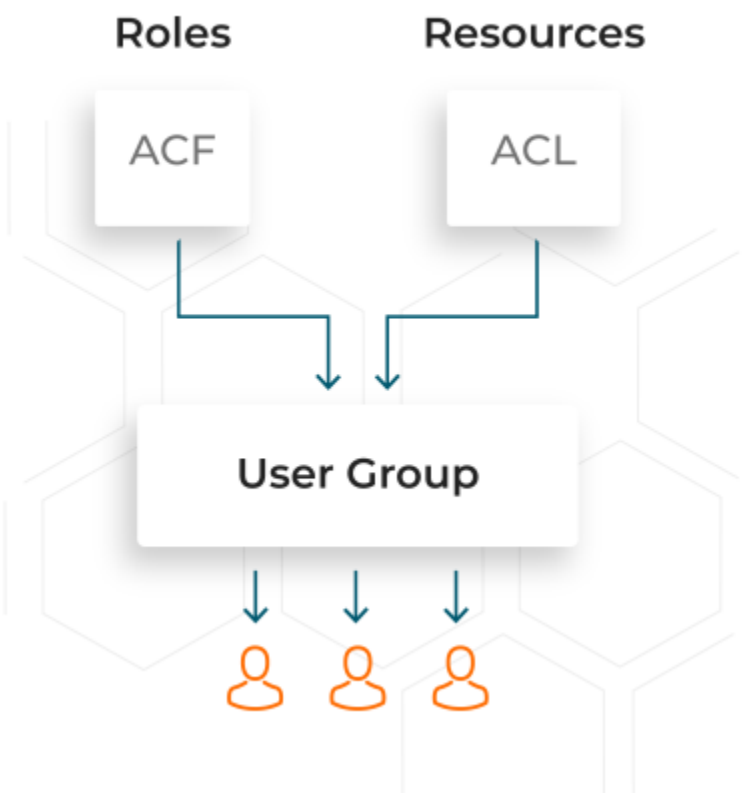
Log forwarding implies forwarding log data from our AppViewX log servers to external hosts like (splunk, elastic) to backup up the data or to process, reporting, monitoring in an external system. The user has to define which type of log data needs to be forwarded and in which format. Audit, AppViewX, and ADC logs can be forwarded. Supported protocol - TCP, UDP.

For more details and Kafka configuration in AppViewX, see Platform User Guide.

Chapter 7: Account

Account Overview

AppViewX offers comprehensive support for Role and Resource-Based Access Control (RBAC). It allows you to integrate with the existing identity stores such as Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) to enforce authorization policies. Roles and Resources can be customized to suit any organizational structure and user requirements.



Role-Based Access Control

Role-Based Access Control (RBAC) is key to eliminating working in silos. AppViewX advanced ADC automation and orchestration platform customizes roles at a very granular level, assigns authorized functions to a specific role, and specifies device and application access to users.

Once you have deployed the ADC in your infrastructure, you have to onboard users with different levels of permissions to control the operations. ADC helps you with a completely customizable Account module to create users, roles, user groups, and resources. Also, it provides the default recommended roles and permissions as per industry standards that can be cloned and customized as required.

Authentication

The **Settings** > **General** tab enables you to configure and manage authentication for

1. **Lightweight Directory Access Protocol (LDAP)**: LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight client-server protocol for accessing directory services, specifically X. 500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.
2. **LDAPS (LDAP over SSL)**: Also known as LDAP over TLS and LDAP over SSL, LDAPS allows for the encryption of LDAP data (which includes user credentials) in transit when a directory bind is being established, thereby protecting against credential theft.
3. **TACACS**: TACAS is a CISCO proprietary system utilizing a transmission control protocol (TCP). In TACAS, the entire authentication packet is fully encrypted and allows us to set up our own CISCO independent servers and databases. The AppViewX system allows you to add more than one Terminal Access Controller Access-Control System (TACACS) server for authentication.
4. **RADIUS**: RADIUS, which stands for "Remote Authentication Dial-In User Service", is a network protocol that controls user network access via authentication and accounting. The AppViewX system allows you to add more than one Remote Authentication Dial-In User Service (RADIUS) server for authentication.
5. **SAML**: SAML stands for Security Assertion Markup Language. It is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP). The AppViewX system allows you to add more than one Security Assertion Markup Language (SAML) server for authentication.

For detailed configuration, refer to Platform User Guide.

On the successful configuration of Authentication protocol in AppViewX, start importing user groups from AD or create manual user groups.

User

A user is an individual who has access to AppViewX using a unique username and password maintained internally or by an external enterprise server such as Active Directories (AD).

Note:

- Administrators can define how users should be authenticated to AppViewX. User authentication can either be an internal authentication or external authentication via LDAP, RADIUS, TACACS, and Single Sign-on.
- To create user accounts, you must be assigned the Administrator role.
- You must add a user to the user group as the roles and resources cannot be directly associated with the user.

In the User page, the following actions can be performed:

- **Create a User**: Create new users and associate them with user groups.
- **Modify a User**: Modify the existing user.
- **Delete a User**: Delete the existing user.
- **Enable a User**: Enable an existing user to activate the user.
- **Disable a User**: Disable the existing user to temporarily deactivate the login.
- **Import User**: Import the list of existing users. if needed the sample template file can be downloaded, which is in .csv format.

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

User Group

A user group is a group of individuals that have access to the same roles and resources. User Groups can be created manually or synced from an active directory or can be bulk uploaded using a spreadsheet.

When you associate a role and resource with a user group, the users within that user group are granted all of the role's and resource's corresponding privileges and permissions.

You can associate roles and resources only with user groups

In the User group page, the following actions can be performed:

- Create a User Group: Create a user group with basic information and associate Roles and Resources to it.
- Modify a User Group: Modify a user group by adding, removing, or modifying the Roles and Resources on demand. The associated users of the user group will be reflected with the changes made to the user group.

- Delete a User Group: Select the required user group and delete the same. You cannot delete a user group that has active users in it. Users belonging to the deleted user group cannot log into AppViewX.
- Clone a User Group: The clone user group option allows you to create an exact copy of an existing user group with a different name. You can modify the roles and resources association while cloning a user group.
- Enable a User Group: Enable the required user group.
- Disable a User Group: Disable the required user group temporarily. You cannot disable a user group that has active users in it and users who are associated with a disabled user group cannot log in to AppViewX.

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

AppViewX encourages users to use the “quick config “option made available to import user groups seamlessly from AD. Following are the Action that can be performed on the User Group:

- Add New User GroupAdd New User Group by Sync Groups from LDAP option:
  1. Click on the Menu Button and Navigate to **Account** > **User Group** > **Quick Config** option.
  2. Authentication stage part of RBAC Configuration wizard flow displayed by default.
  3. Navigate to the User group stage as part of the RBAC Configuration wizard flow.
  4. Click the **Add new group** button.
  5. Select ‘Sync groups from LDAP’ option.
  6. Click **Proceed**.
- Add New User Group by TACACS/RADIUS/SAML/AppViewX option:
  1. Click on the Menu Button and Navigate to **Account** > **User Group** > **Quick Config** option.
  2. Authentication stage part of RBAC Configuration wizard flow displayed by default.
  3. Navigate to the User group stage as part of the RBAC Configuration wizard flow.
  4. Click the **Add new group** button.
  5. Select ‘TACACS/RADIUS/SAML/AppViewX’ option.
- Add New User Group by Bulk Import option:

1. Click on the Menu Button and Navigate to **Account** > **User Group** > **Quick Config** option.
2. Authentication stage part of RBAC Configuration wizard flow displayed by default.
3. Navigate to the User group stage as part of the RBAC Configuration wizard flow.

4. Click the **Add new group** button.
5. Select **Bulk Import** option

Role

Each role assigns a specific set of permissions relating to the modules that can be accessed and the tasks that can be performed in each AppViewX module. The roles can be assigned only to a user group. The user groups that are assigned with a role will automatically inherit all the associated permissions. User groups can be assigned with more than a role.

The Roles management of Inventory comprises some of the Out of the Box (OOB) roles available for ADC. The OOB roles can be cloned, enabled, and disabled. It can not be updated or deleted. Administrators can also create custom roles. Custom roles can be updated, deleted, enabled, and disabled. Users can either use OOB roles (if match their needs) or custom roles to map to user groups. The available roles are:

- **Application Manager ADC**: The application manager will have complete/partial (complete access will not be given to Shared devices) insight on all the application-related devices. The application manager gets “write” access to all the objects of application objects.
- **Auditor ADC**: Auditor access is predominantly for archived logs and the backed-up data along with the current reports and log data which would be used for all kinds of activity tracing.
- **DevOps ADC**: The user can automate, execute workflows, perform plugin management and upgrade.
- **Executive Director ADC**: Executive access is more towards business-level operational smoothness. The success rate of the changes and the monitoring data for the critical devices in report form ensure adequate details to have respective vendors communicate more data-oriented. This role would also help in understanding failure patterns.
- **Network Manager**: Access to complete infrastructure as the responsibility of access provisioning to users and the limited device access provisioning is also handled by this user only. It would require almost admin level of access on the infrastructure, would only not include core system-level access.
- **Traffic Manager**: The traffic manager can manipulate the state and status of any object/device to which he has been given access, there are possibilities that users may not have access to all the objects in the device as most devices are based on a shared network infrastructure basis.

In the **Roles** page, the following actions can be performed:

- **Create a Custom Role**: Create a custom role. Note that to assign functions at a more granular level, click the expand icon beside a function checkbox and then select individual sub-options within that function. In the image below, for example, you can select ADC, which automatically assigns all six sub-options and the sub-sub-options within them, or you can expand the ADC function and select only the sub-options or sub-sub-options you want to assign.
- **Modify a Role**: Modify a role in AppViewX.

> **Note:** The Out of the box role functions can not be edited. Only custom roles functions can be edited.

- **Delete a Role**: To delete a role from AppViewX.

Note: You can not delete a role that has active users in it. Also Out of the box (OOB) roles cannot be deleted. Only custom roles can be deleted.

- **Clone a role**: The Clone a role option allows you to create an exact copy of an existing role with a different name. The user can modify the permissions and tasks that can be performed while cloning a role.
- **Enable a Role**: Enable a role in AppViewX.
- **Disable a Role**: Disable a role in AppViewX. Note that You cannot disable a role that has active users in it and The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.
- **Role Mapping to User groups**: To map a role to user groups.

For detailed instructions to perform above-mentioned actions, see Platform Userguide.

Resources

All the devices and objects that are configured within AppViewX are termed as Resources. The resource allows you to specify access at a granular level across all the devices and modules of AppViewX listed in this section, where the permission definitions are independent of each other. The resources can be assigned only to a User group. The users that are assigned to the user groups will automatically inherit the permissions associated with that resource. User groups can be assigned with more than one resource.

In the **Resources** page, the following actions can be performed:

- **Create Resources**: Create Resources with ADC devices and objects in R or RW permissions
- **Modify Resources**: Modify Resources by adding, removing, or modifying permissions on devices and objects.
- **Delete Resources**: Delete Resources. Users associated with the deleted resources will not be able to access the Application.

AppViewX can be configured to not only provide permission to specific devices in the inventory but also to specific objects (Virtual server, Pool, Servers) within the device. This helps you to create custom user roles according to their need limiting the access by making sure the unauthorized access to critical objects is limited.

AppViewX gives you the flexibility to create users with various permission levels to access devices and objects. One is **Read only (R)** where users are allowed to access devices or objects to only view the configuration without permission to modify it. The second level of permission is **Read & Write (RW)**, where users have the access to both views and modify the device or object configuration.

AppViewX encourages users to use the **quick config** option made available to streamline the user creation process and help users identify the true potential of RBAC.

Using the **Quick config** option, you can perform the following actions:

- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query using object/Certificate fields available within AppViewX.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates using a script to tag based on data available with external tools (SNOW, Other CMDB, etc.).
- Rule templates are pre-shipped to ease the rule creation to dynamically tag resources
- Dynamically created resources can be assigned to user groups dynamically by mapping the respective rule to the required user groups as part of the Rules in Use inventory in the wizard flow.
- Manage the order of execution for the RBAC rules.
- Manage short circuit options to dynamically tag ADC objects.

For assigning the devices or objects to resource, refer to the following sections:

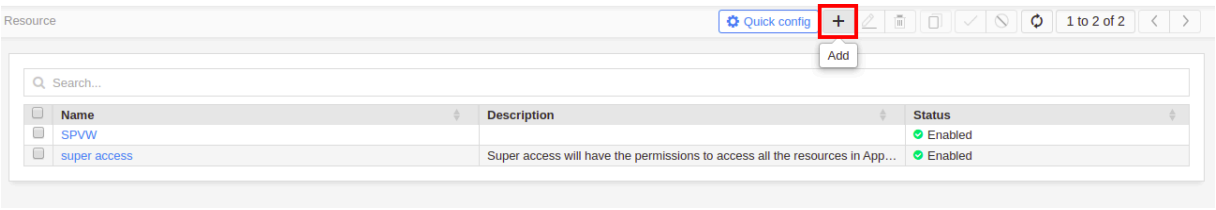
- Assign Devices to Resource
- Assign Objects to Resource

You can also check the following video link for more details:

https://www.appviewx.com/use-rbac-eliminate-working-silos/

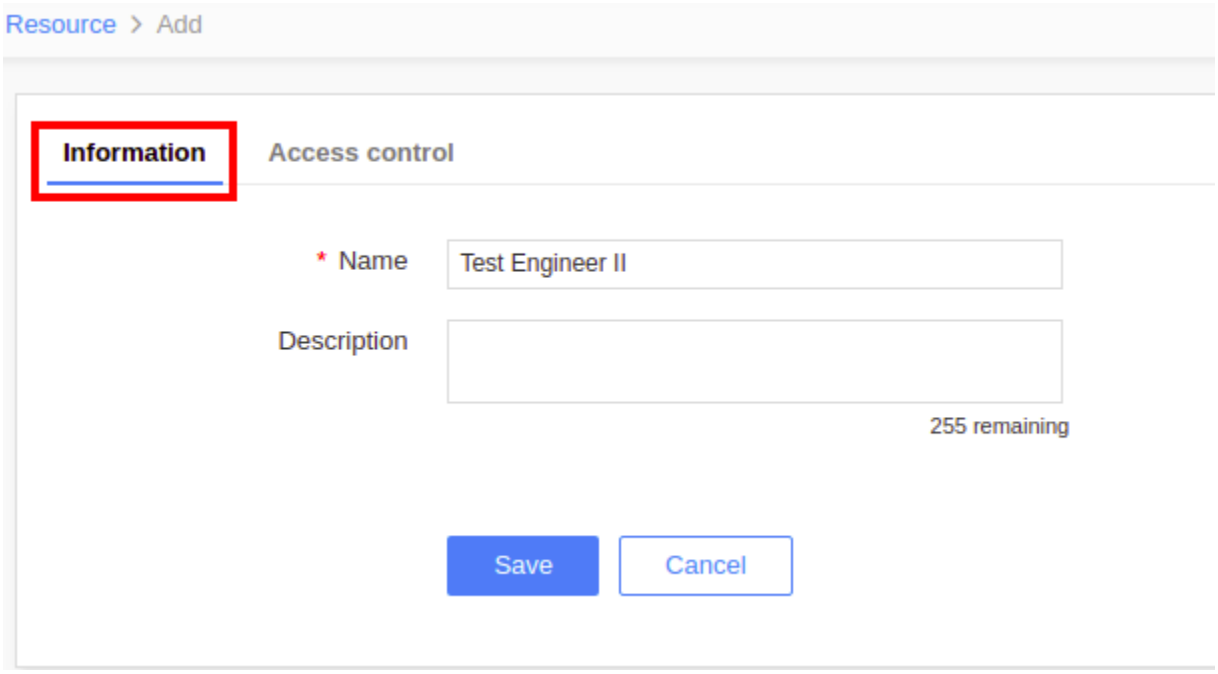
Assign Devices to Resource

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Account** > **Resource**.
3. Click on the Add (+) icon to navigate to the resource addition page.

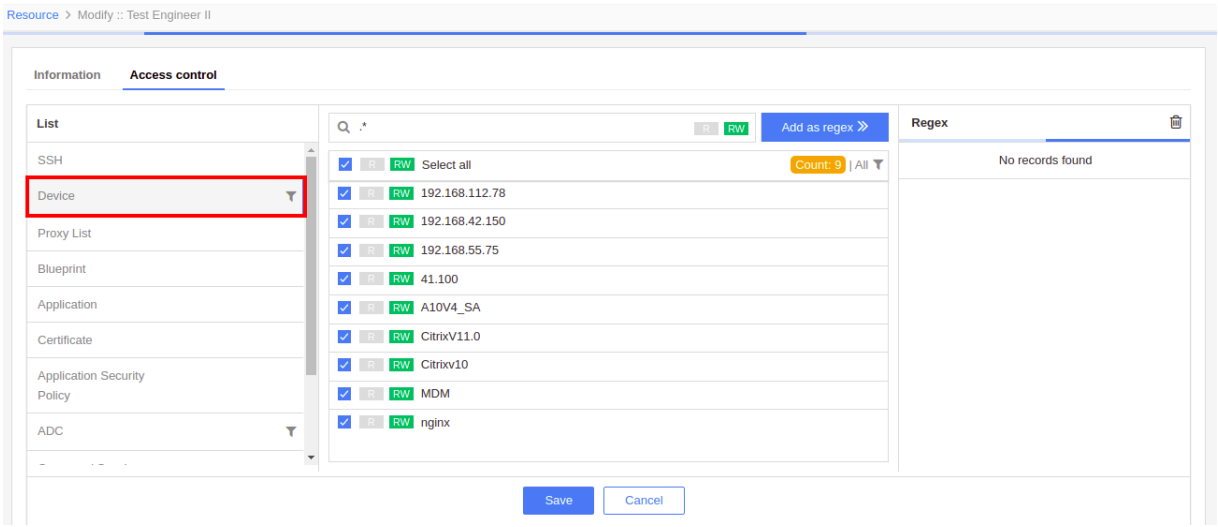


4. From the Resource Add page, configure the group details as given below and click Save.

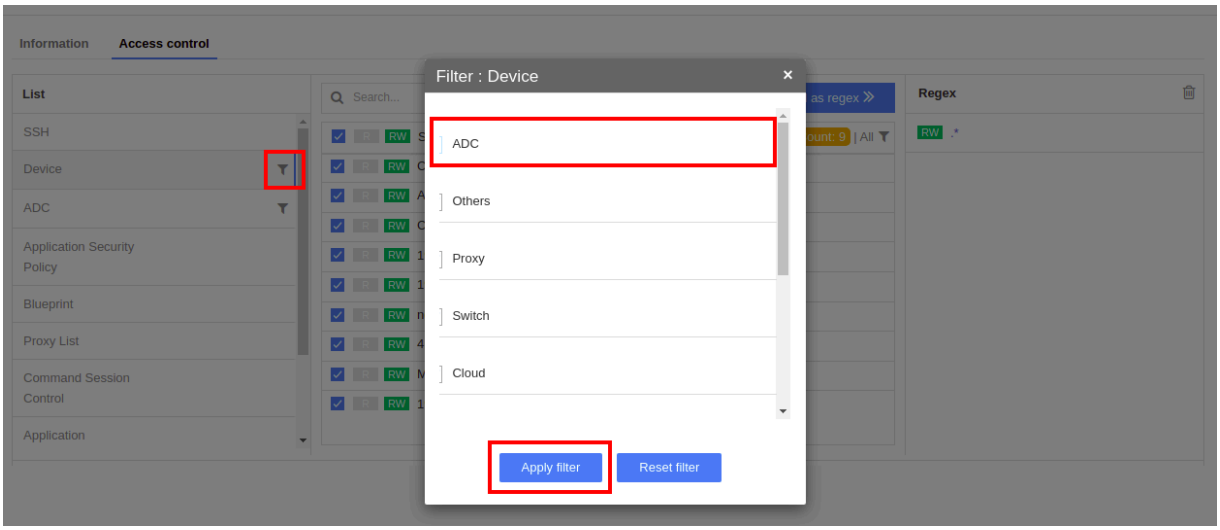
Field	Type	Mandatory	Description	Validation
Name	Text	Yes	Name of the resource to be added.	Resource name cannot be empty.
Description	Text	No	Description of the resource.	A maximum of 255 alphanumeric characters and space are allowed.



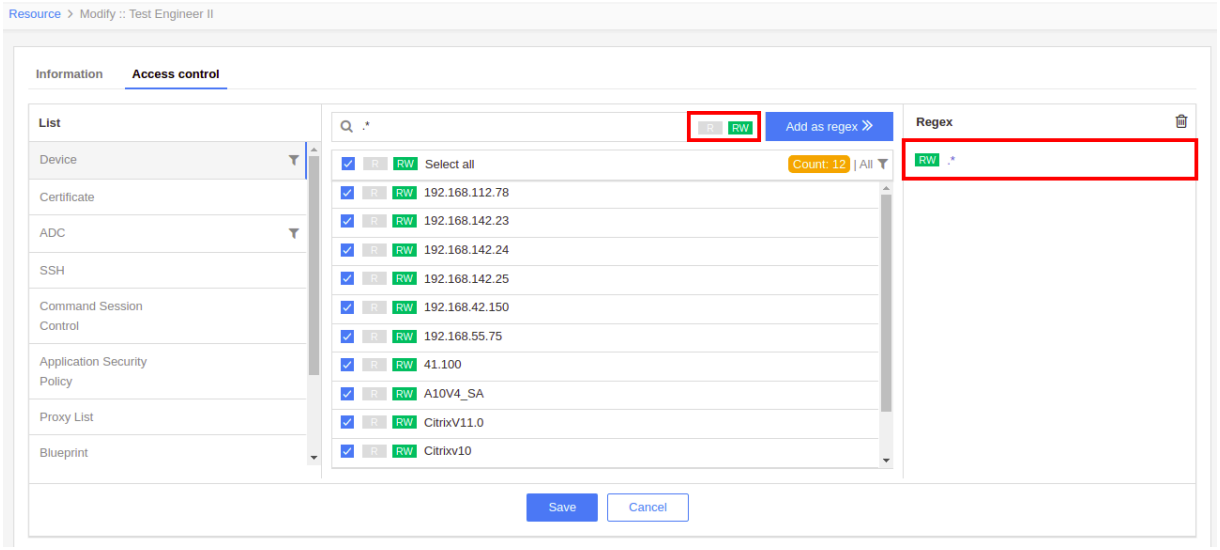
5. From the Resource Access control page, select Device from the list in the left panel.



6. Select the filter icon, select ADC in the filter list and then click **Apply Filter**.



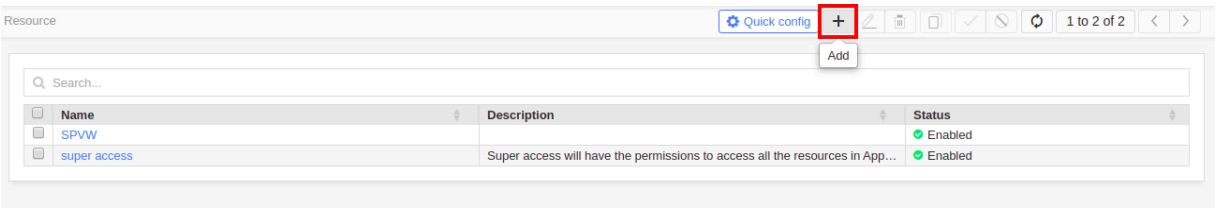
7. Search for the regex of the device name(s), provide R/RW permission, and click Add as Regex to assign the device(s) to the resource.



8. Click **Save**.

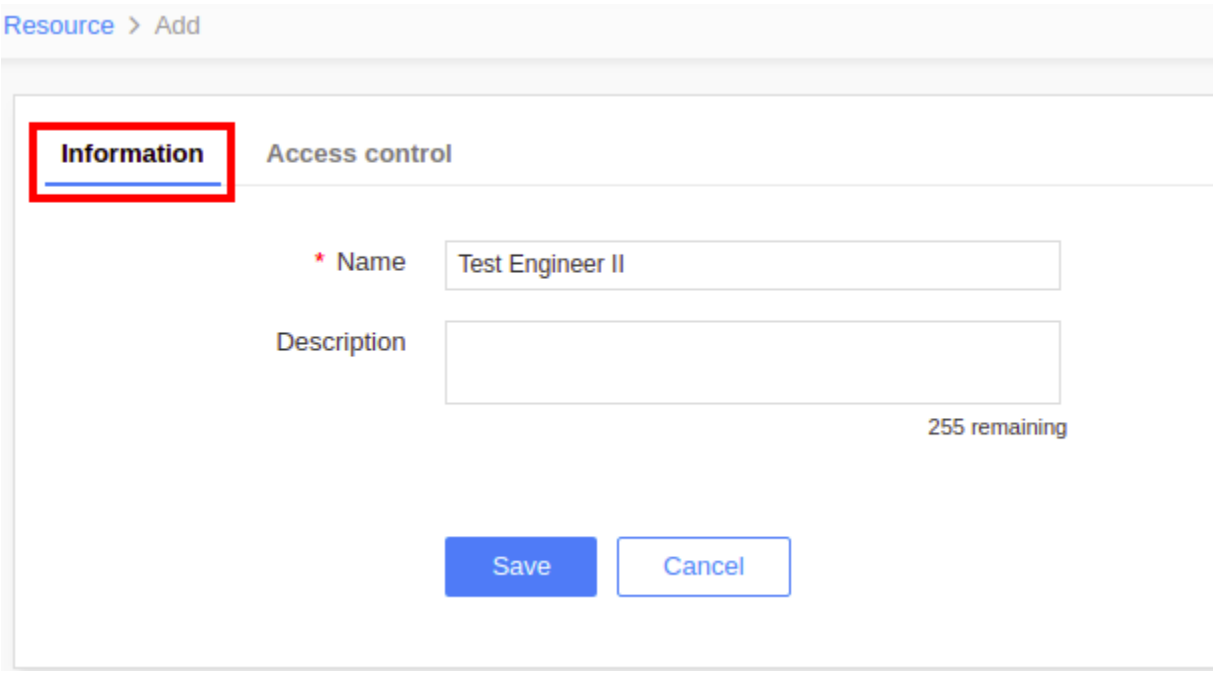
Assign Objects to Resource

1. Log in to the AppViewX application with valid credentials.
2. Select **Menu** > **Account** > **Resource**.
3. Click on the **Add** (+) icon to navigate to the resource addition page.

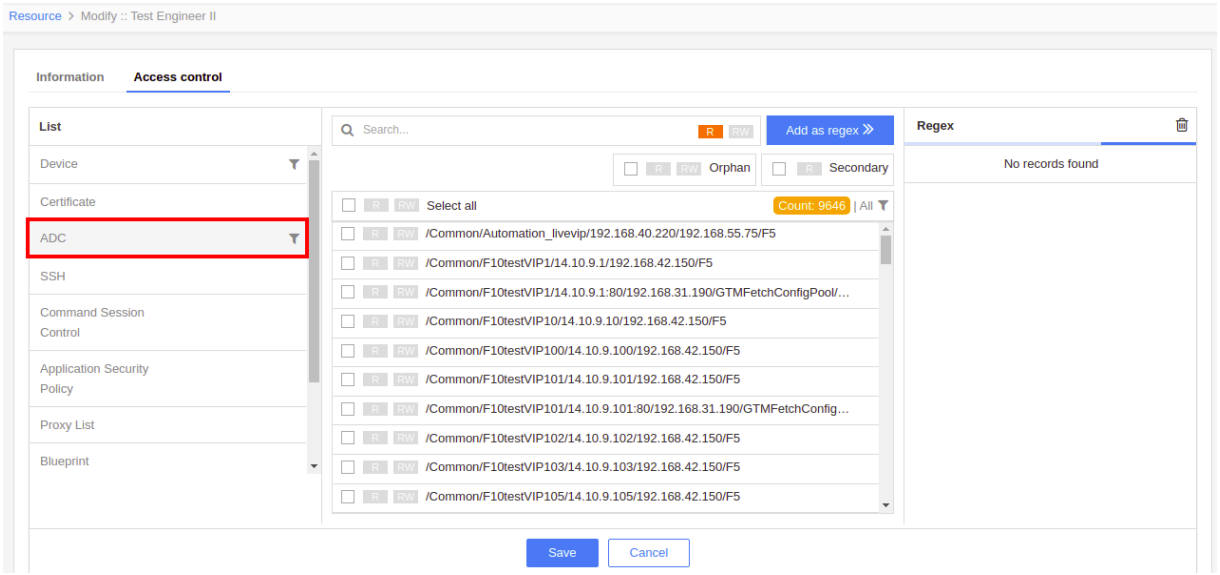


4. From the Resource Add page, configure the group details as given below and click **Save**.

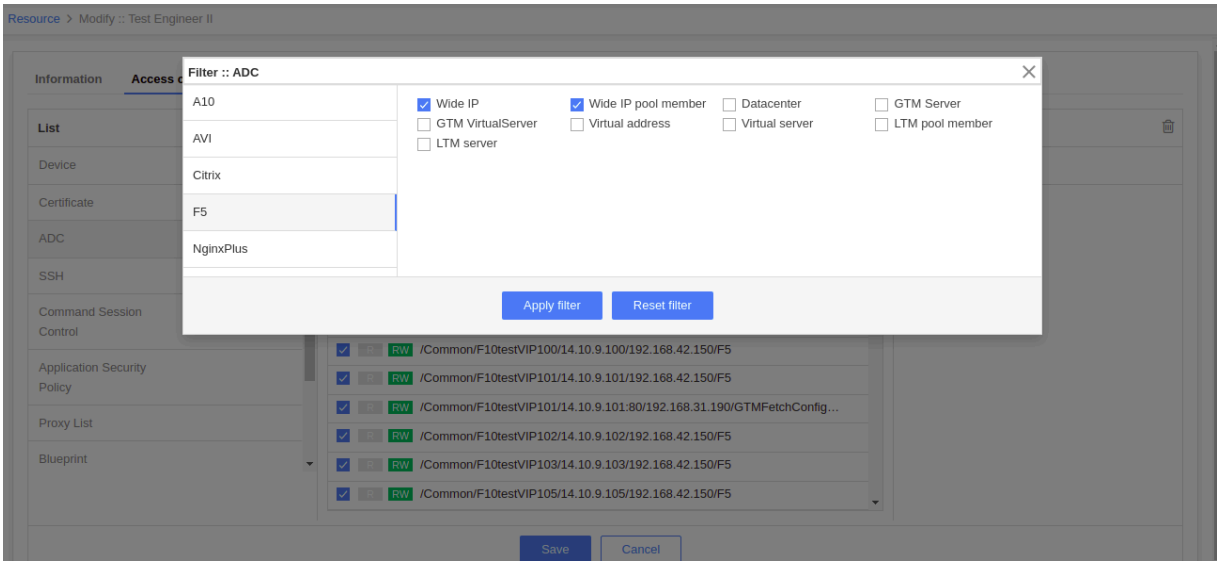
Field	Type	Mandatory	Description	Validation
Name	Text	Yes	Name of the resource to be added.	Resource name cannot be empty.
Description	Text	No	Description of the resource.	A maximum of 255 alphanumeric characters and space are allowed.



5. From the Resource Access control page, select ADC from the list in the left panel.



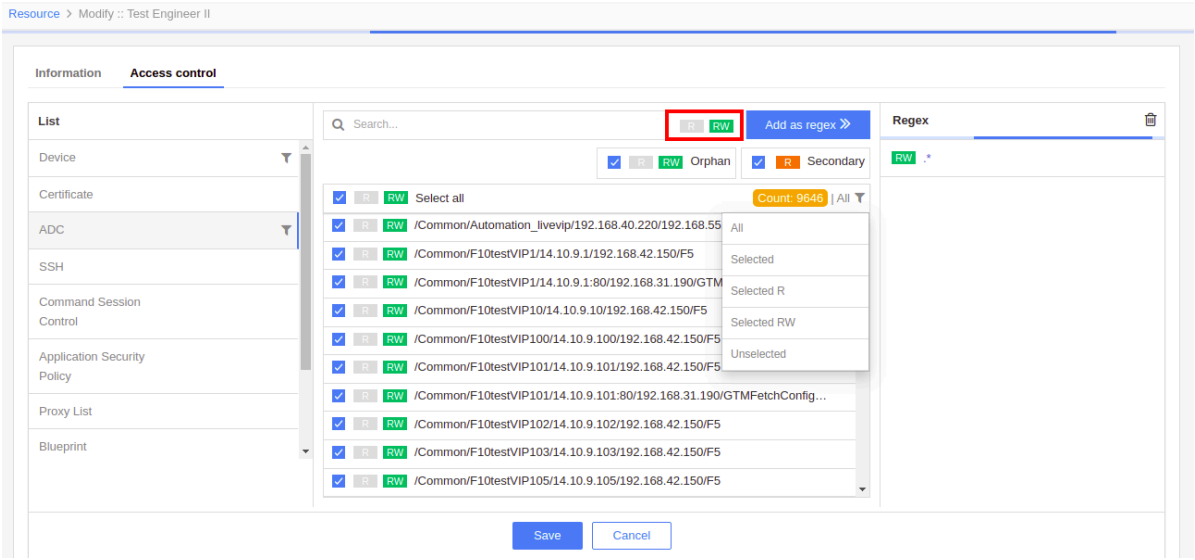
6. Select the filter icon, select the ADC vendor in the filter list and the object type(s), and then click **Apply Filter**.



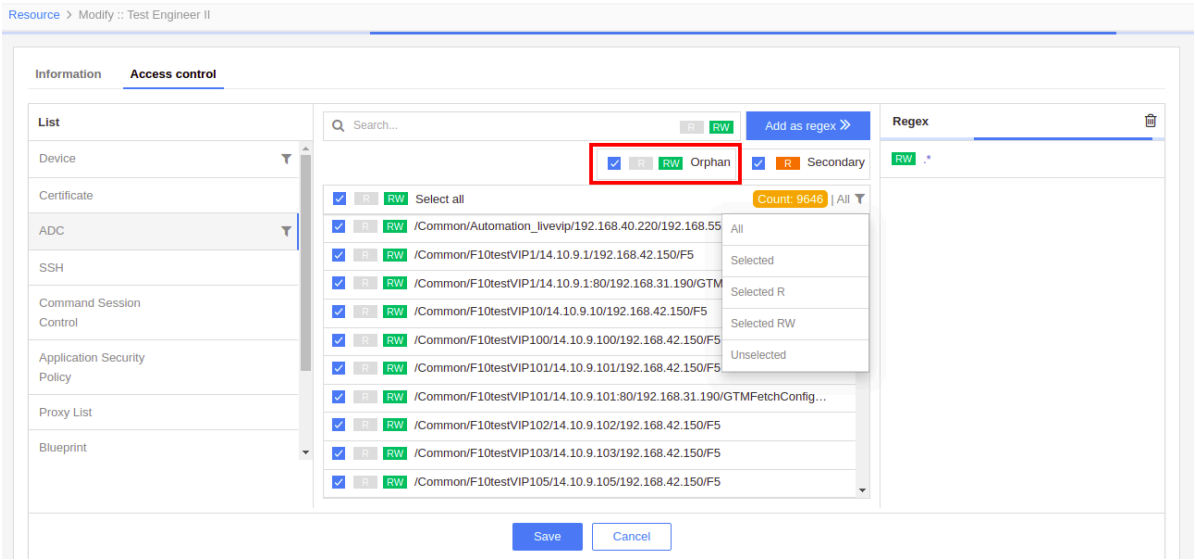
Note: For F5 devices, the LTM Class object type is also displayed and by selecting this object type, the permission for class objects can be managed. The applied permission for the class objects from here will reflect in Dashboard, Control Center, and Restore/Compare.

7. Search for the regex of the object display name(s).

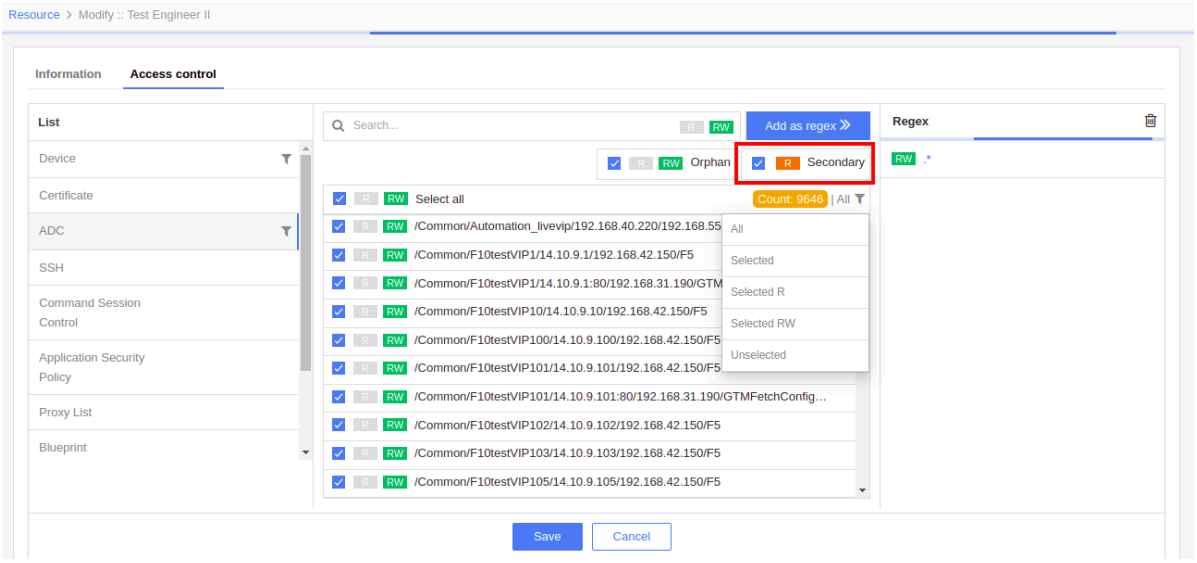
- Select R/RW permission for the object(s).



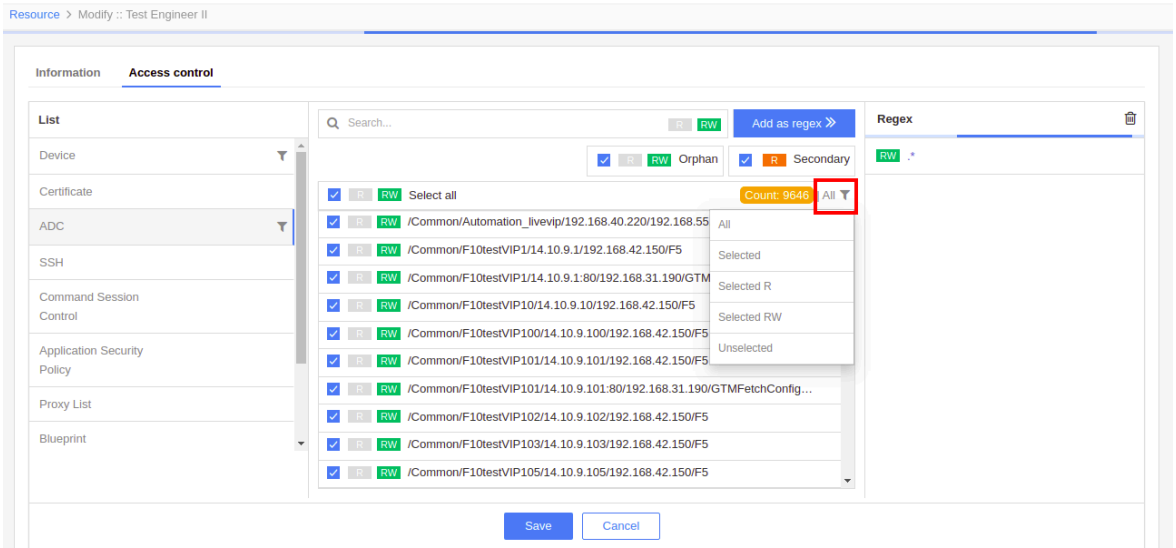
- Select R/RW permission for the orphan object(s)(optional).



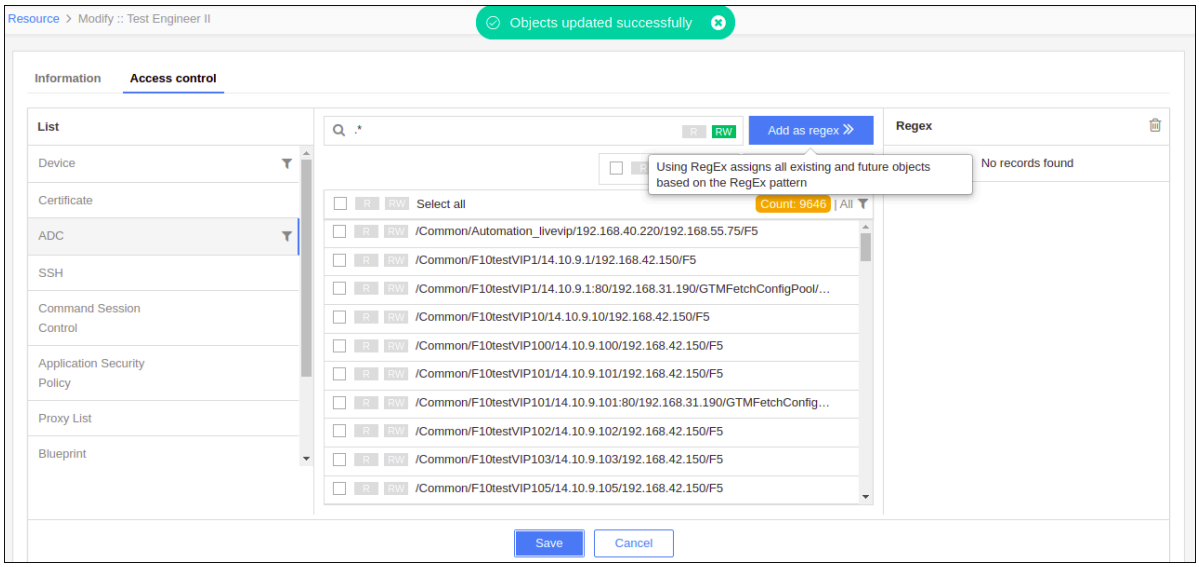
- Select R permission for the secondary object(s)(optional).



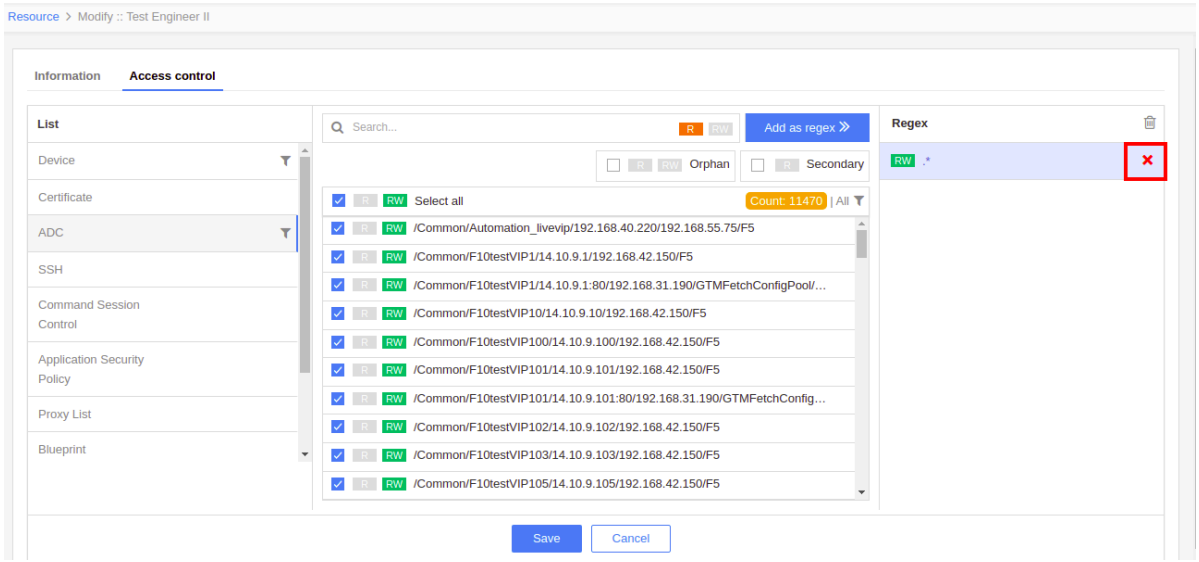
- Click the ALL filter icon to filter the objects based on the given permission.
  - Click All to get all the objects.
  - Click Selected to get the objects with any permission.
  - Click Selected R to get the objects with Read permission.
  - Click Selected RW to get the objects with Read/Write permission.
  - Click Unselected to get the objects without any permission.



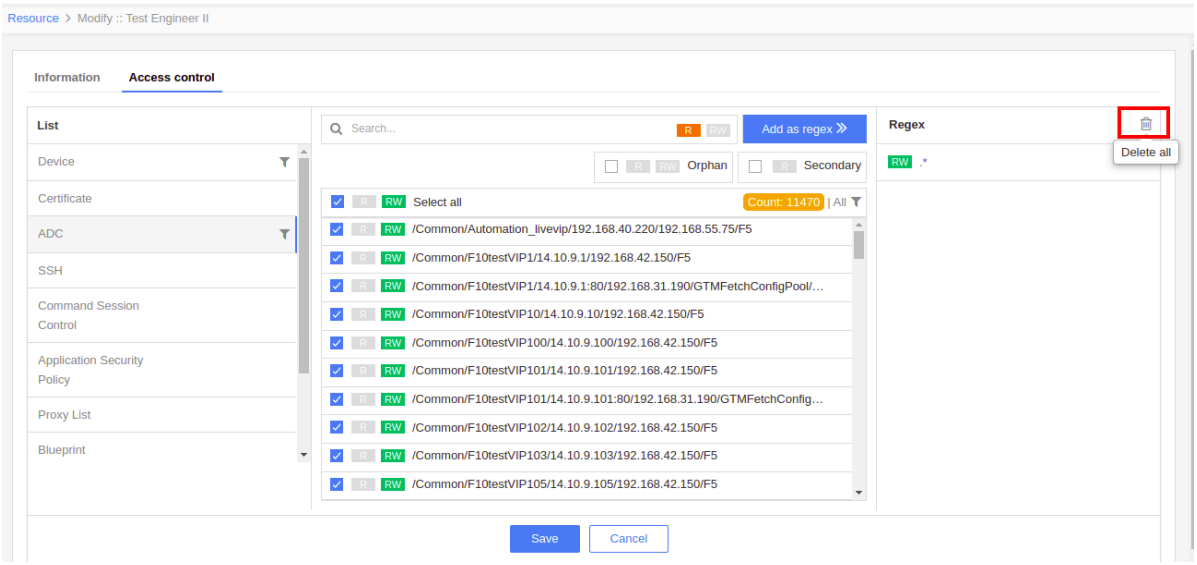
- Click Add as Regex to assign the objects(s) to the resource.



• Click the cross icon to delete any regex from the resource.



• Click the delete icon to delete all the regex from the resource.



8. Click **Save**.

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, the **Quick Config** wizard flow option has been introduced in the existing Authentication, User groups, Roles and Resources. Using the **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 log in to AppViewX.
- Add users groups into AppViewX by pulling specific user groups from AD into AppViewX based on specific patterns/keywords/codes and support the 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 a script and assigning permissions to user groups dynamically.

Accessing the 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.

To configure role-based access control, the user should have ACF permissions. With ACF permission, you can:

- Assign devices to resource
- Assign objects to resource

Chapter 8: Studio

- Studio

Studio

Studio Overview

This chapter covers the major features and functionality of the AppViewX Studio module, which is a platform that can be used for the following purposes:

- Building custom workflows and tasks to make network operations agile
- Performing decision-based automation to achieve single or zero-touch provisioning
- Automating tasks using a third-party integration
- mention the OOB workflows for ADC that are available.

The Studio module is divided into three sub-systems, each of which has its own set of tasks you can perform:

- **Workflow** - It comprises of the following:
  - **Design** a custom workflow using a drag and drop UI or Import an existing workflow.
  - **Variables & Hooks** - Execute custom REST or script codes on top of the existing code using the **Hooks** section. You can define **Magicvariables** (static or dynamic), which are similar to the global variables. The only difference is that the global variables can be used only within one workflow, whereas magic variables can be used across workflows. The hooks can also be mapped with the magic variables.
  - **General** - Add/manage Python codes and regular expressions using the **Helper script** and **Regex Library sections** respectively. You can access the AppViewX **GitHub** repository containing various reusable workflows.

For more detail, refer to Visual Workflow Guide (link).

- **Reports** - It comprises of the following tabs:
  - **My reports** contain all the reports created by you or all the reports that have been created, depending on the permissions you have been assigned. It allows you to create, clone, or delete report(s).
  - **Store** allows you to view or clone 31 (6 samples and 25 certificates) pre-built reports.

For more detail, refer to Reports Guide.

- **Rules** - Allows you to create an action (force down, enable, and disable) related rule(s) to trigger workflows for the ADC objects.

For more detail, refer to Visual Workflow Guide (link).

- **Pages** - AppViewX provides a one-stop portal with all the service offerings in the form of low code pages to enable self-servicing for the end-users (like App owners, Network Engineers, CA, Admin, etc.) in a simplified and intuitive manner. There are Out of the Box catalogs and as well option to customize catalogs as per the organization standards. Access the opinion through **Menu** > **Studio** > **Pages**.
  - **Benefits**

- An intuitive self-service portal to access all service offerings for employees, and partners via Single Pane of Glass.
- Customer Experience – Users only see services that are available to them, described in business terms they understand.

- Build your own App catalog/portal.

- Configurable Catalog page that allows for personalized task views
- Low Code designer portal – Low Code and configurable toolsets, allowing users to brand Catalog solution so it feels familiar and intuitive for the end-users.

For more detail, refer to Pages User Guide.

Rules

Rules Inventory helps to define custom business rule(s) for specific actions and workflow(s) can be invoked for closed-loop automation.

Users can customize any action as per the business use case using workflow and associate it with the actions. The workflow will be triggered for a Rule-based on the criteria configured.

Key Features:

- A common Rule Inventory integrating key platforms (i.e., Control Center, Device Management, Alerts, Insight, etc.).
- Provision to define custom business rule(s) for module-specific actions.
- Provision to define the trigger, rule criteria for module-specific actions.
- Provision to define one or many workflow actions against a rule.
- Provision to execute the specific action defined based on the pre-defined rule.
- Provision to trigger workflow requests/token ID, and indicate the relevant status.
- Provision for a common notification center for actioning workflow requests.

Why Rules, Policy in AppViewX?

A policy is a condition that when met causes the system to perform a specific set of actions. Policies can be used for event-driven automation and to automate network change and configuration tasks such as:

- A comprehensive policy/rule inventory to define, manage policies, and triggers.
- Web interface to configure business data objects without changing code.
- Eliminates hard coding of complex business logic; enables faster policy-driven GTM solutions.
- Define internal rules across modules – Certificate, Alert, Control Center, Dashboard, Device Management, Reports, etc.
- Perform event-driven orchestration based on internal and external event(s).
- Provision to map Business processes to specific actions across AppViewX.
- Detecting and collecting configuration changes made by external users.
- Notifying users and systems when a configuration change is detected.
- Auto-remediating critical compliance violations.
- A rule can be a server-side, client-side logic that runs when any CRUD operation is performed.

The Rules sub-system within the Studio module allows you to perform the following tasks:

- Create a rule
- Clone a rule
- Delete a rule

Clone a Rule

To clone a rule,

1. Click **Menu** > **Studio** > **Rules**.
2. The **Rules** screen displays a list of all the rules.
3. Select the rule you want to clone.
4. From the **Actions** dropdown, click **Clone**.
5. In the screen that appears, enter a **Name** for the cloned rule.
6. Click **Enable** to clone the rule in an enabled state. Alternatively, you can click **Save As Draft** to save the cloned rule to the AppViewX system and enable it later on.

Create a Rule

To create a rule using the Rules sub-system in the Studio module,

1. Click **Menu** > **Studio** > **Rules**.
   A list of rules is displayed.
2. Click **Create Rule**.
3. In the **Rule Name** box, enter a name for the rule.
4. (Optional) In the **Description** box, enter additional information about the rule.
5. (Optional) Select the location/entity where the rule must run and the action upon which the rule must be triggered.
6. (Optional) Select the specific action on a page where the rule has to be executed. The action could be Enable or Disable.
7. Associate a workflow against the Rule. AppViewX provides default Action execution workflows that integrate with Service NOW for change management. You can associate a default workflow or custom workflows.
8. (Optional) Define the **Rule criteria**.

> **Note:** The default workflows are available in the Studio >Workflows> Rules category. AppViewX allows to clone and customize the default workflows.

Delete a Rule

To delete one or more rule(s),

1. Click  **Menu** > **Studio** > **Rules**.
2. The **Rules** screen displays a list of all the rules.
3. Select the rule(s) you want to delete.
4. From the **Actions** dropdown, click **Delete**.
5. In the Confirmation dialog box that appears, click **Yes**.

Chapter 9: SETTINGS

- SETTINGS

SETTINGS

Settings Overview

Appviewx's ADC Settings helps manage the Device and Object specifications related to Configuration synchronization, Report, and Statistics.

Device Settings

The device settings can be configured in the following tabs:

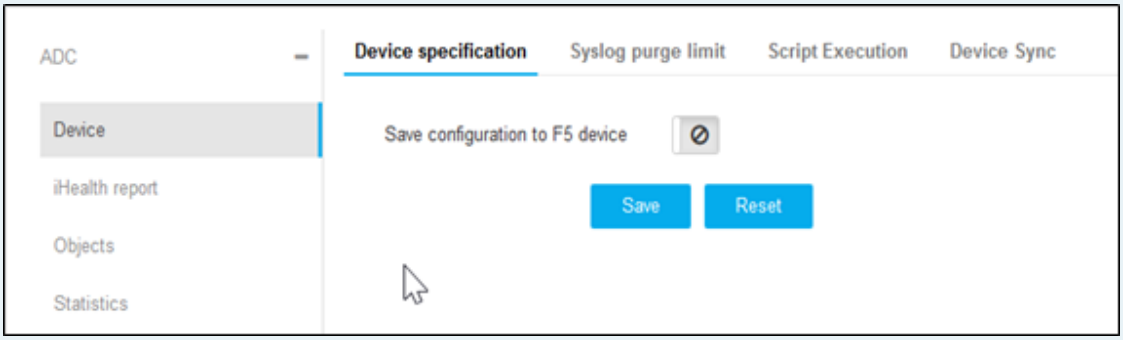
Device Specification Tab

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.

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**.

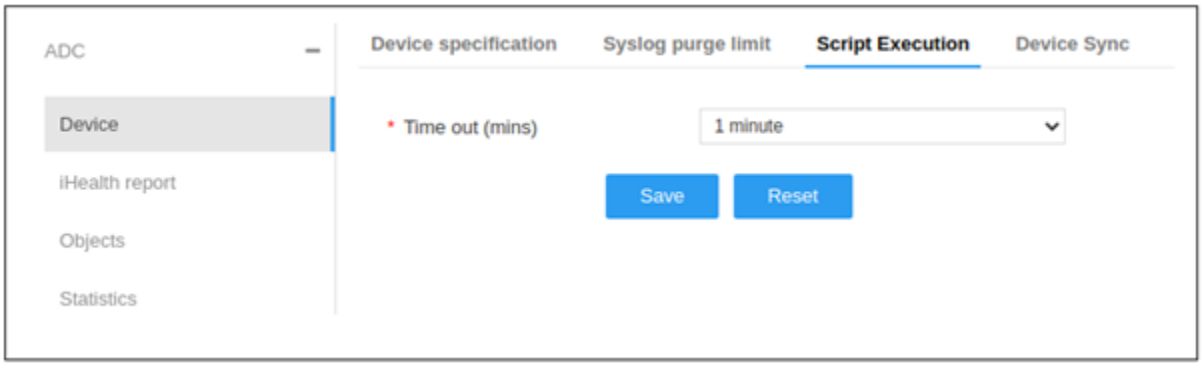
> **Note:** To reset the changes, click Reset.

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**.

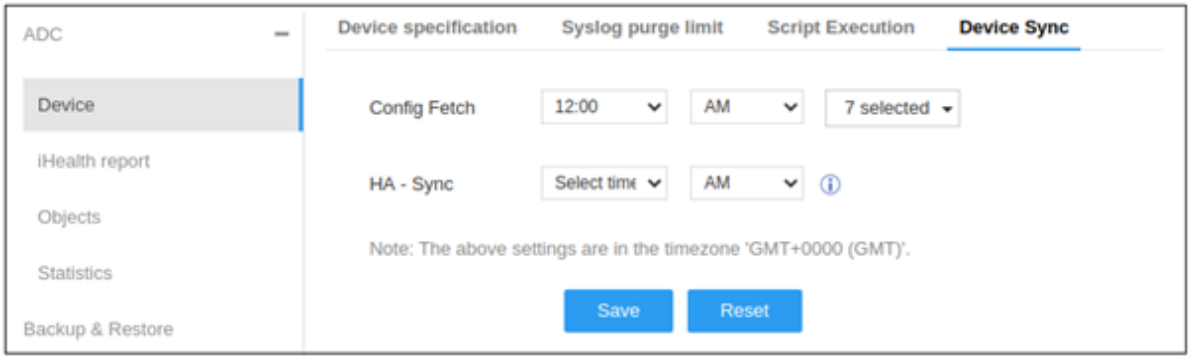
Device Sync

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:

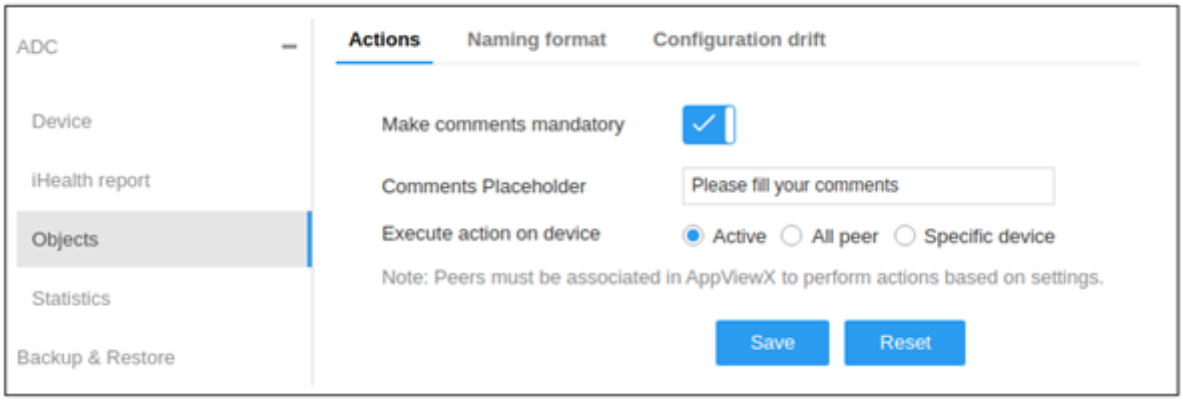
- Actions
- Naming Format
- Configuration drift

Actions Tab

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**.

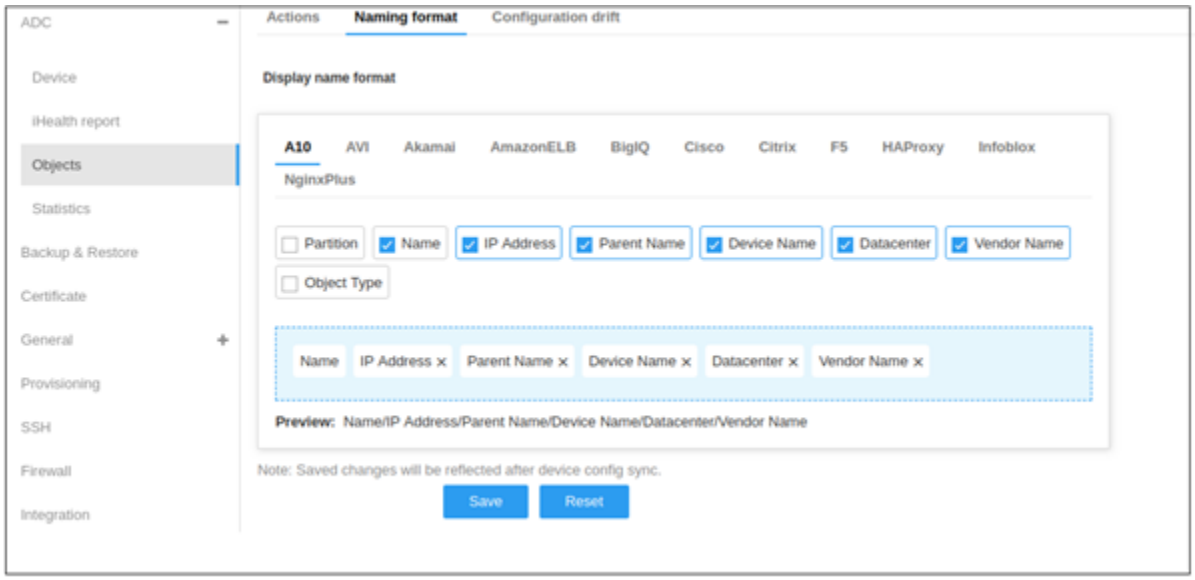
> **Note:** To discard the changes, click **Reset**.

Naming Format Tab

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**.

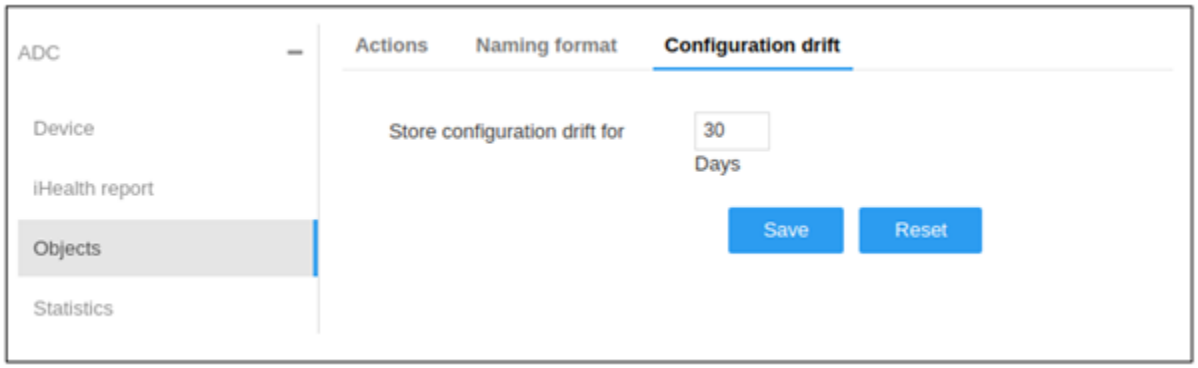
> **Note:** To discard the changes, click **Reset**.

Configuration Drift Tab

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**.

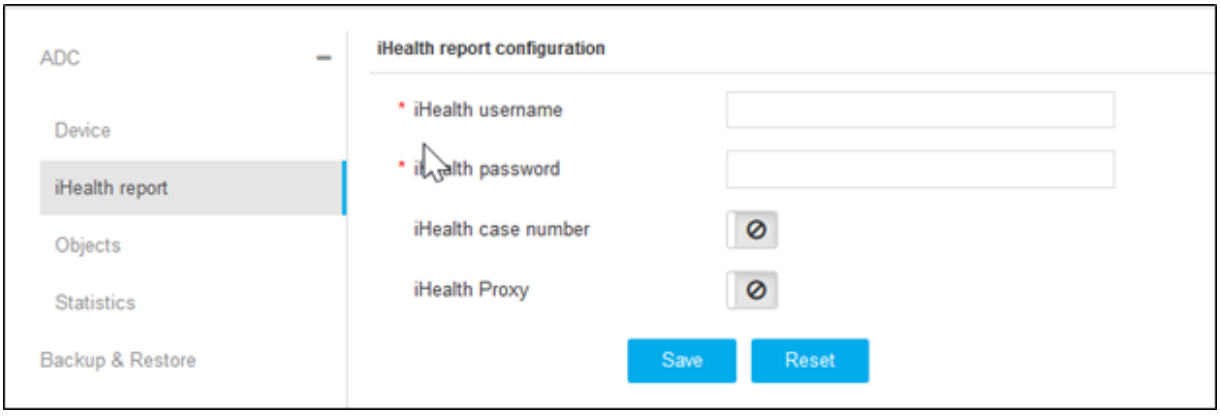
> **Note:** To discard the changes, click Reset.

iHealth Report

Configure health portal information for a vendor to generate iHealth reports of devices.

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**.

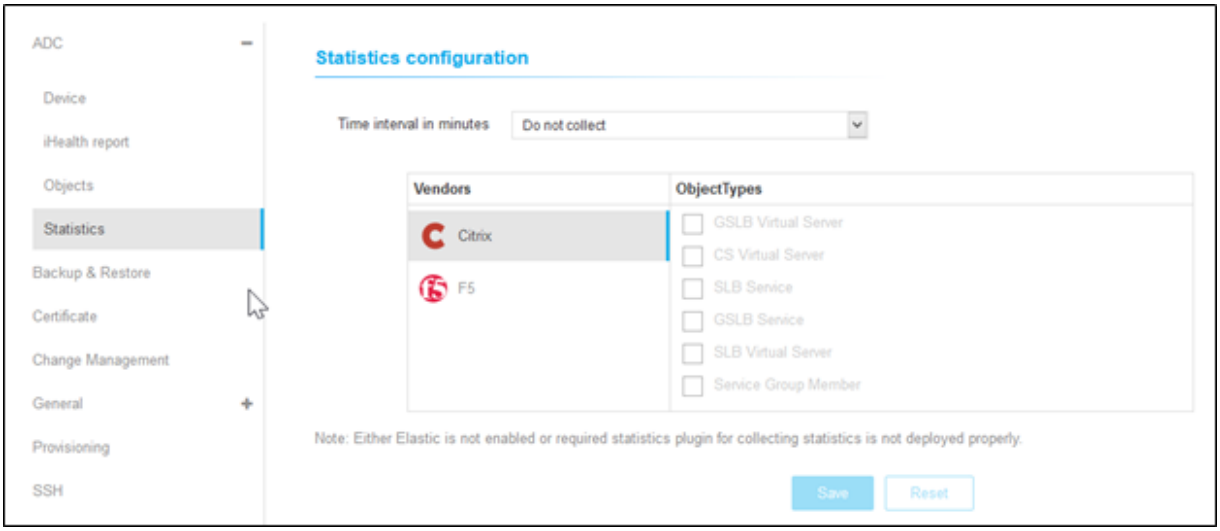
> **Note:** To discard the changes, click **Reset**.

Statistics Settings

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.

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 choose the object types from the list for which statistics must be fetched from the device.
4. 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**.

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: Glossary

This table describes the common terms used in this guide.

Terms	Definition
LDAP	LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight client-server protocol for accessing directory services, specifically X. 500-based directory services.
Object	Objects are traffic management entities configured in the devices that are responsible for load balancing the traffic. Eg: A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. For a given network, there are usually multiple objects functioning. Some object types - WideIP, Virtual Server, Pool, Pool Member, Irule, Monitor, Profile, Policy, etc.,
OOB Workflow	A workflow defines a logical flow of activities or tasks from a Start event to an End event to execute a specific service. AppViewX ships predefined Out of the Box (OOB) workflows that allow application teams to take ownership and self-service their applications.
Resource	Resources are the devices and objects that are configured within AppViewX.