appviewX

# User Guide

**Version: 2020.1.0**

# Copyright AppViewX, Inc.



## Trademarks



## 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 2020.1.0 | 14 Feb 2020 |

## About this Guide

Welcome to the complete guide to getting started with AppViewX. This guide describes the various modules and functionalities offered by AppViewX.

## Audience

This guide is intended for network/IT Operations, engineers, DevOps and Security Operations using AppViewX for the first time with an understanding of the networks. It aims to introduce basic concepts related to building self-service Pages for Line of Business, employees and partners.

This guide is intended for the following audience:

- PKI
- Application Teams
- Network Operations (NetOps)
- Security Operations (SecOps)
- Network Engineers

## Text Conventions

The following text conventions are used in this document:

| Convention | Description |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in the text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `codeblock` | Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter. |

# Chapter 1: Common Tasks



## Overview

This chapter covers tasks that are common to many, if not all, of the modules with AppViewX. Because the instructions apply to multiple screens within AppViewX, they do not tell you how to navigate to the location from which you will be performing each task: it is assumed that you are already on the relevant screen.

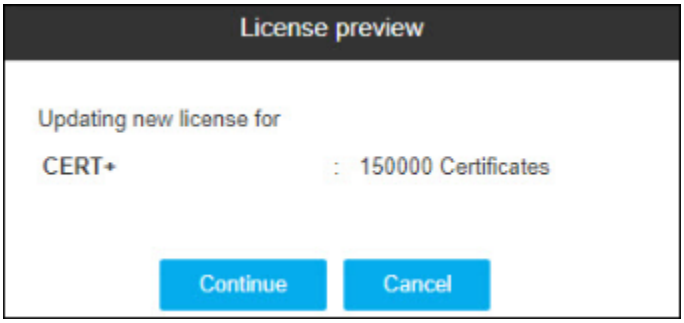
# Upload an AppViewX License

The following steps explain how to upload a new AppViewX license into the system. For details on how to upgrade an existing license, refer to the Upgrade an AppViewX License section of this guide.

To upload a new AppViewX license:

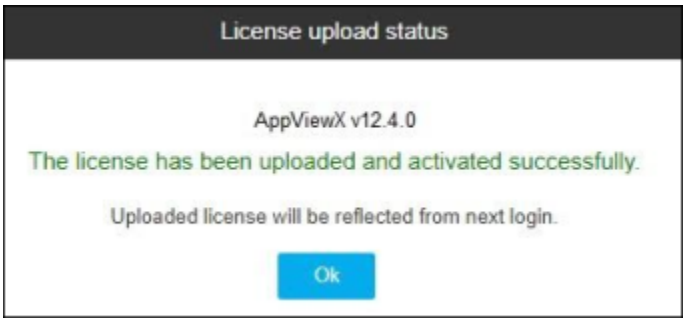
1. Log in to AppViewX using the default credentials you were given by your administrator.
2. On the **Upload License** screen that appears, click **Browse** and then locate and select the license file.


3. As soon as you select a file, the **Upload** button becomes active. Click it to begin the upload process. The screen then displays a license preview screen listing the modules that you have purchased and the license limits and counts for each.


4. Click **Continue**.

5. As soon as the license is done being uploaded and activated, the screen displays the message: **The license has been uploaded and activated**.



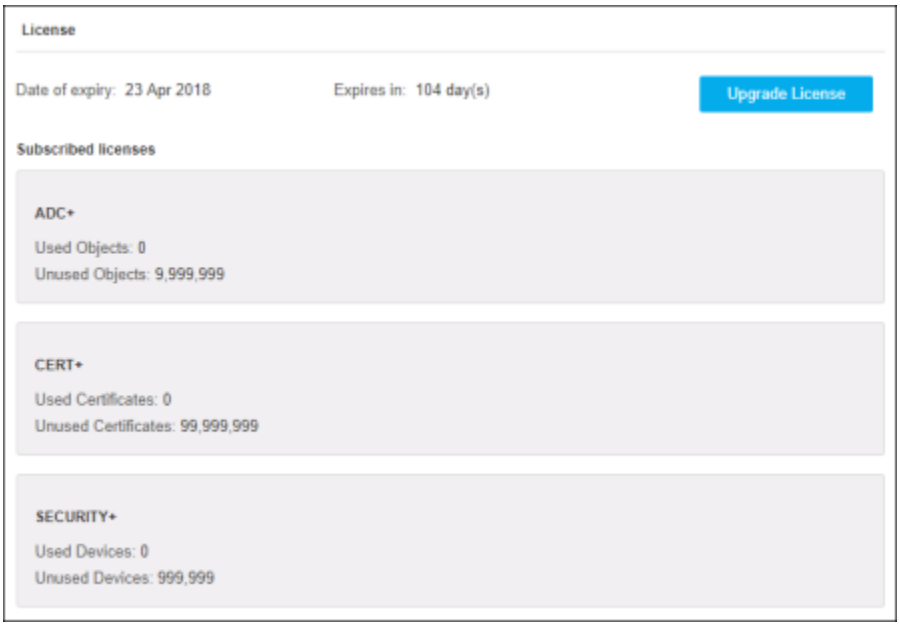

6. Click **OK** to return to the login screen. When you log in again, your new license will be active.
   - If the license is uploaded and not activated, the screen displays the following message: **The license has been uploaded successfully, but the activation has failed. For more information contact AppViewX support**.
   - If the license upload is failed, the screen displays the following message: **The license upload has failed, try uploading it again**.

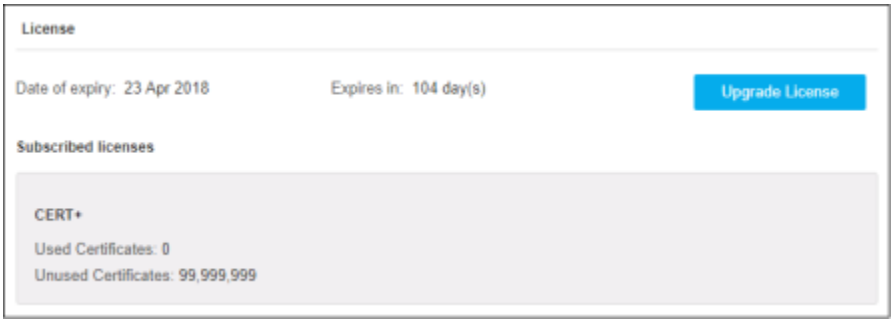
## Upgrade an AppViewX License

The following steps explain how to upgrade an existing AppViewX license. For details on how to upload a new license, refer to the Upload a License section of this guide.

To upgrade an existing AppViewX license:

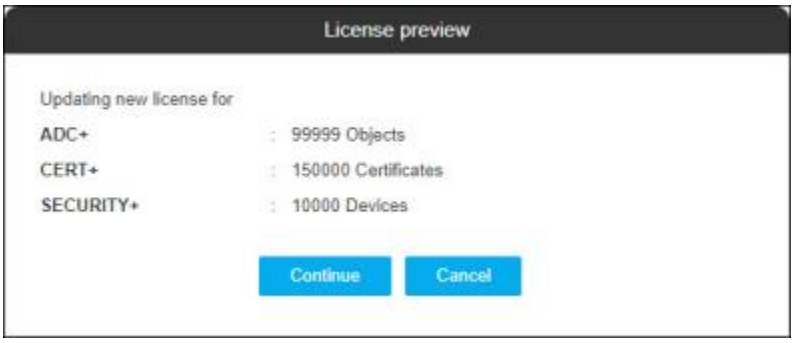
1. Click ☰ and select **Settings** > **General**.
   The **License** screen appears, showing details about the main license and all subscribed licenses.

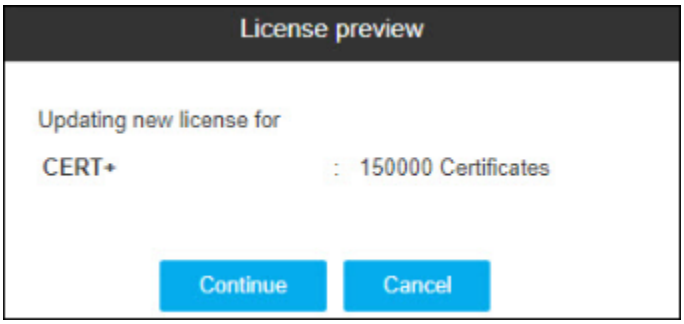



2. Click the **Upgrade License** button.
3. On the **Upload License** screen that appears, click **Browse** and then locate and select the license upgrade file.

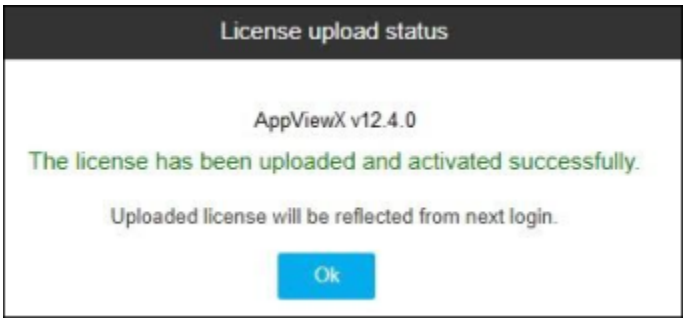

4. As soon as you select a file, the **Upload** button becomes active. Click it to begin the upload process. The screen then displays a license preview screen listing modules that you have purchased and the license limits and counts for each.




5. Click **Continue**.

   As soon as the license is done being uploaded and activated, the screen displays the message: **The license has been uploaded and activated successfully**.



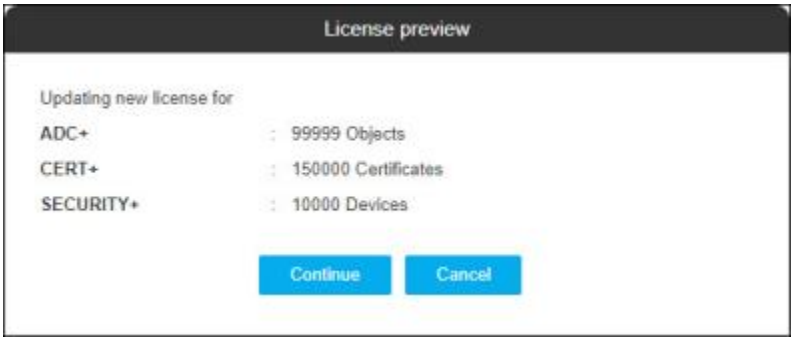

6. Click **OK** to return to the login screen. When you log in again, your newly upgraded license will be active.
   - If the license is uploaded and not activated, the screen displays the message, **The license has been uploaded successfully, but the activation has failed**. **For more information contact AppViewX support**.
   - If the license upload is failed, the screen displays the message, **The license upload has failed, try uploading it again**.

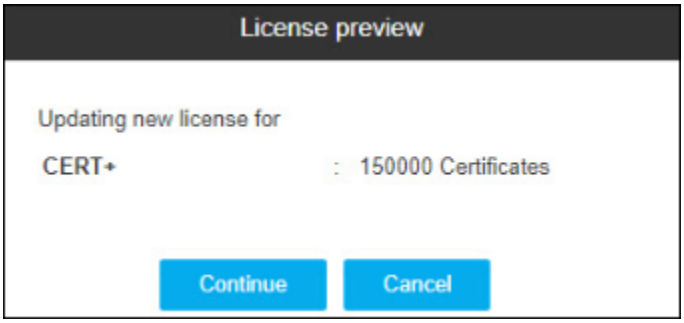
# Renew an AppViewX License

To renew an AppViewX license:

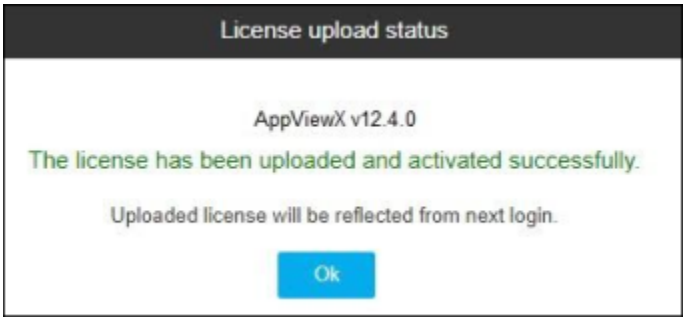
1. Log in to AppViewX using the default credentials you were given by your administrator.
2. If the license is about to expire or if the license limit has been exceeded, you will be prompted to renew the license from the **License Status Intimation** screen.
3. Click **Renew License**.
4. On the **Upload License** screen that appears, click **Browse** and then locate and select the license file.


5. As soon as you select a file, the **Upload** button becomes active. Click it to begin the upload process. The screen then displays a license preview screen listing the modules that you have purchased and the license limits and counts for each.



6. Click **Continue**.
   As soon as the license is done being uploaded and activated, the screen displays the message, **The license has been uploaded and activated**.




7. Click **OK** to return to the login screen. When you log in again, your newly upgraded license will be active.
   - If the license uploaded is not activated, the screen displays the message, **The license has been uploaded successfully, but the activation has failed**. For more information contact AppViewX support.
   - If the license upload is failed, the screen displays the message, **The license upload has failed, try uploading it again**.

## Change the User Account Password

The internal users can set up a new password by providing the current password for theirAppViewX user account. Also, the user who has access permissions for all other user accounts can reset their AppViewX user account password.

To change the password:

1. Click ☰ on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, click **Admin**.
3. On the **User Information** screen that appears, click **Change Password**.
4. Enter the current password for the user account that you want to change.
5. Enter and then confirm the new **password** in their respective fields.
6. Click **Change** to update the password.
7. You need not click the **Save** button on the **User Information** page to update the password.

## Reset the Password

To reset the password:

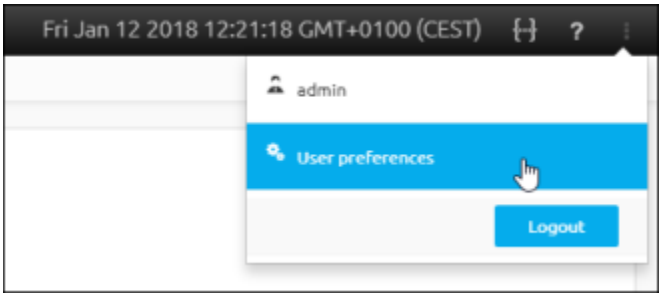
1. Click and select **Settings** > **General**.
2. Click the in the Command bar.
   The **Modify** screen appears.
3. Click **Reset password**.
4. On the **Reset password** screen that opens, enter and then confirm the **new password** in their respective fields.
5. Click **Change** to update the password.

> **Note:** You need not click the **Save** button on the **User Information** page to reset the password.

# Change the Language of the AppViewX Interface

To change the language of the AppViewX interface:

1. Click on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, select **User Preferences**.



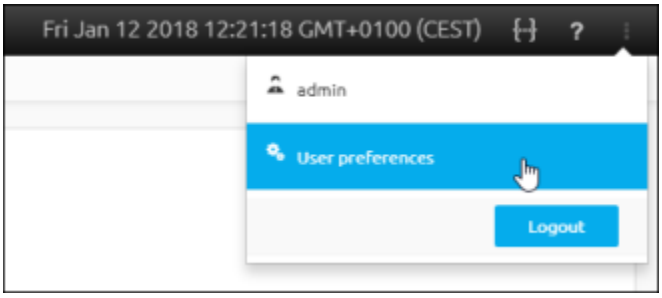

3. On the User Preferences screen that appears, click the **Select Language** dropdown and choose the language you want the AppViewX interface to display:
   - English
   - French
   - Portuguese
4. Click **Save**.

# Change the Theme of the AppViewX Interface

The term "theme" refers to the colors used throughout the headings, buttons, menu items, and page divisions within the AppViewX interface. At present, there are two options: Blue & Black or Green & Black.

To change the theme of the interface:

1. Click ☰ on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, select **User Preferences**.

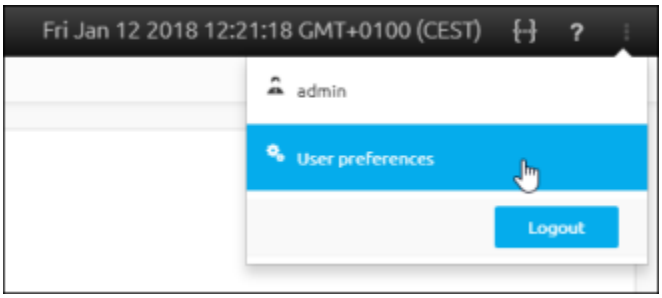



3. In the **Theme** field on the **User Preferences** screen that appears, click the theme you want to switch to.
4. Click **Save**.

# Change the Font of the AppViewX Interface

To modify the font type and/or font size displayed in the AppViewX interface:

1. Click ☰ on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, select **User Preferences**.

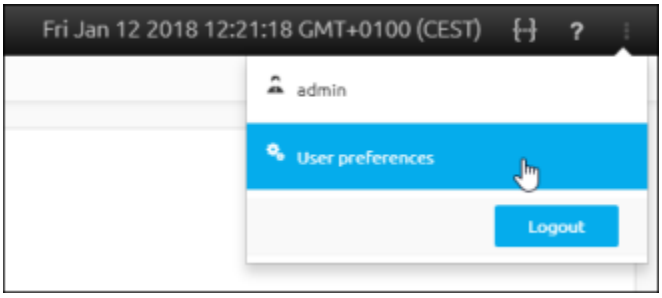



3. On the **User preferences** screen that appears, select the font type you want to use in the AppViewX user interface: Open Sans or Ubuntu.
4. (Optional) In the **Font** display field, click the font size you want to use in the user interface.
5. Click **Save**.

# Change the Date Format of the AppViewX Interface

To modify the date format displayed in the AppViewX interface:

1. Click ☰ on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, select **User Preferences**.

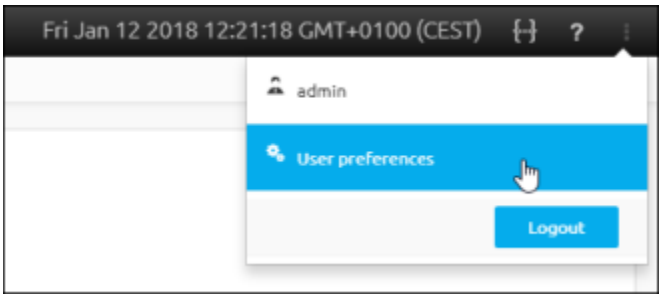



3. On the **User preferences** screen that appears, select the date format you want to use in the AppViewX user interface: MM/DD/YYYY or DD/MM/YYYY.
4. Click **Save**.

# Change the Landing Page of the AppViewX Interface

To modify the landing page of the AppViewX interface:

1. Click ☰ on the top-right of the AppViewX interface.
2. In the dropdown menu that appears, select **User Preferences**.




3. On the **User preferences** screen that appears, select your **Preference** for the landing page of the AppViewX user interface.
4. Click **Save**.

## Refresh a Screen

To refresh the data that appears on a results screen, dashboard, widget, topology, or workflow:

1. Move your mouse to the Command bar.
2. Click  .

## Modify the Layout of a Screen

To modify the types of columns and the order of columns displayed on a screen:

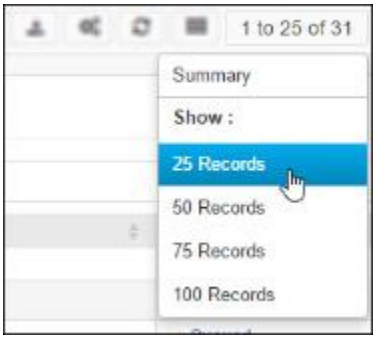
1. Click  in the Command bar.
   A **Columns** screen pops up.
2. In the Available field, click » beside each column you want to add to the screen.
3. In the Selected field, click the « icon beside each column you want to remove from the screen.
4. In the Selected field, click ↑ or ↓ to reorder the column layout.
5. Click **Save**.

## Change the Number of Records Displayed on a Screen

To change the number of records displayed on a screen:

1. Click 

in the Command bar.
2. In the dropdown list that appears, click the number of records you want to be displayed on the screen.




The screen refreshes and displays the number of results you selected.

# Align Objects on a Screen

Few screens in AppViewX, such as topologies and dashboards allow you to click and hold objects and drag them to different locations.

To reset these screens to their default layouts where all objects are arranged uniformly, click the **Align** icon in the Command bar.

**Note:** The appearance of the Align icon varies depending on which screen you are on.

1. On dashboard screens, from the command bar, click  .
2. On topology screens, from the command bar, click  .

All objects on the screen are then arranged uniformly, both horizontally and vertically, with none overlapping.

# Minimize or Maximize an Object

You can minimize and maximize objects on the screen to suit your current needs or to reflect the overall importance of one object compared to others.

To maximize or minimize an object:

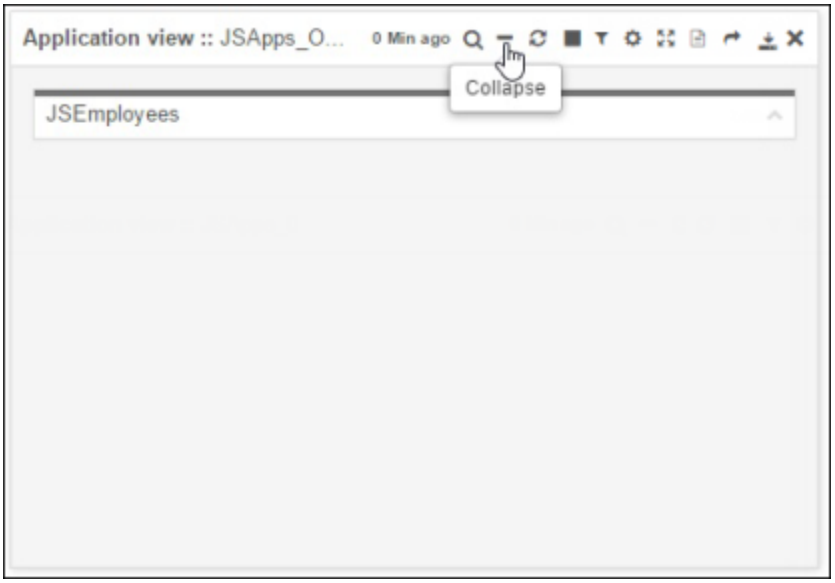
1. Click  in the Command bar.
   The object then stretches to cover the entire width of the screen.
2. To reverse the action, click the  in the Command bar.

# Collapse or Expand an Object

Expanding and collapsing objects differs from minimizing and maximizing them. Collapsed objects display only a header field, all other information is hidden. Minimized objects display all information, but in a smaller area than maximized objects.

To collapse or expand an object:

1. Click ➖ in the Command bar.




The object collapses to display only its header information and the Command bar.


2. To reverse the action, click ➕ in the Command bar.

# Building Reports on Custom Collections

You can now enable/disable the custom Collections to be accessible to reports using the query builder.

## Enable Collection to Build Custom Query

1. Click ☰ and select **Collections**.
2. Select the collection that you want to enable. (You can also select all the collections as a whole).
3. Click 🔗.

   You will now be able to access the collection from the query builder section while creating reports.

## Disable Collection to Build Custom Query

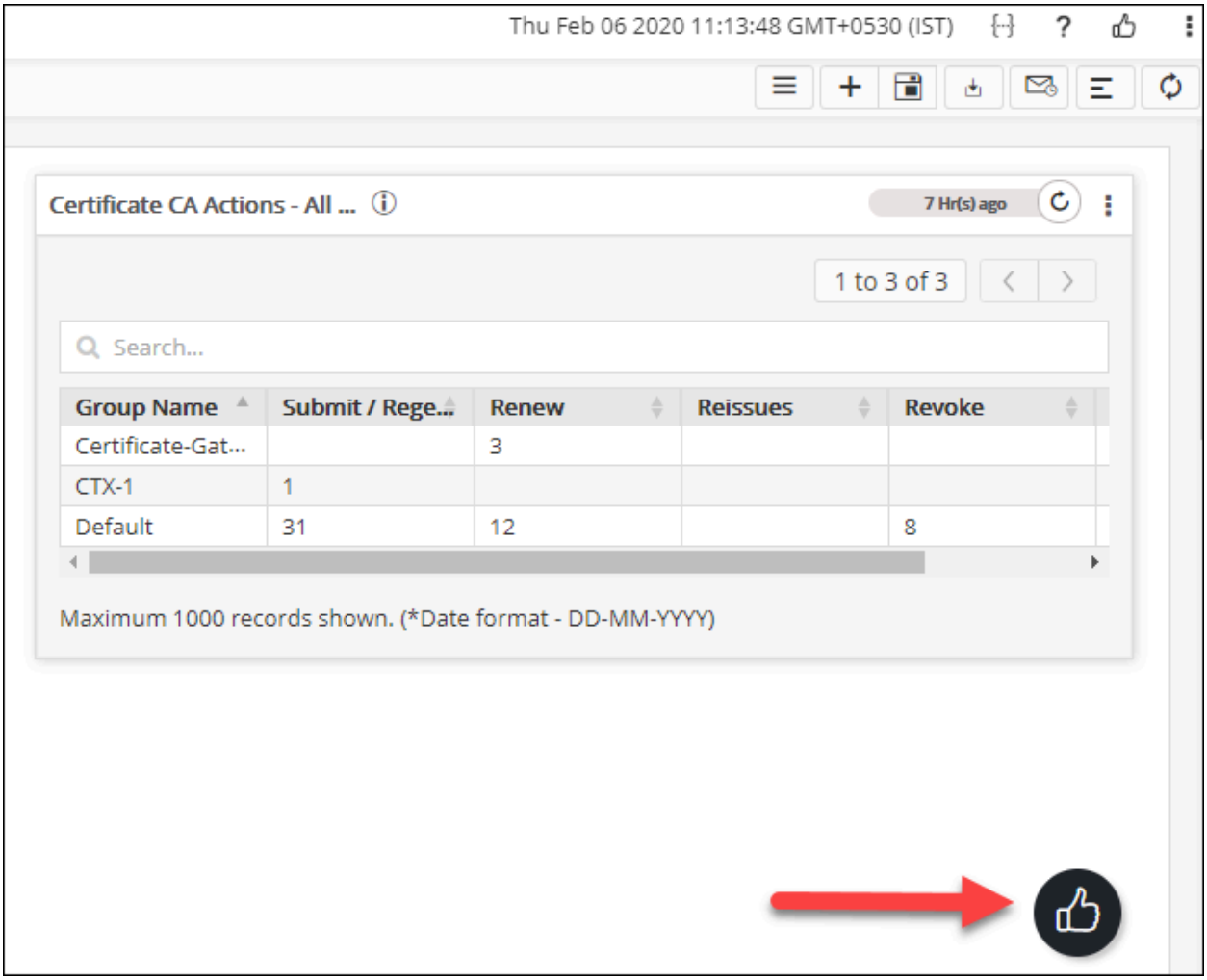
1. Click ☰ and select **Collections**.
2. Select the collection that you want to disable. (You can also select all the collections as a whole).

3. Click  .

   You won't be able to access the selected collections from the query builder section while creating reports.

## User Survey and Feedback

A feedback icon will be displayed at the bottom right and the top right corner throughout the product for the user to submit feedback for the respective module. You can view the user feedback by downloading the User survey and Feedback report from the Reports store.




This option can be disabled by navigating to **Settings** > **General** > **Reports** > **(Enable/Disable) User Survey and Feedback**.

# Chapter 2: Dashboard



## Dashboard Module

The Dashboard module enables the user to manage, monitor, and interpret all the configured applications and their objects. It has been categorized into the following sections:

- **Default** - Displays the pre-defined widgets to provide the AppViewX metric usage reports and up-to-the-minute reports containing statuses and statistics for device, certificates, and SSH managed within the AppViewX platform. Any dashboard can be set as a default one by clicking  beside its name. Within the default dashboard you can do the following:
  - View the reports
  - Create a Custom Dashboard
  - Align the Widgets
  - Save the Dashboard
- **Custom** - Displays all the customizable widgets to provide an overview of all the ADC device and its 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. Within the custom dashboard, you can do the following:
  - Custom Dashboard Tasks
  - Widget Tasks

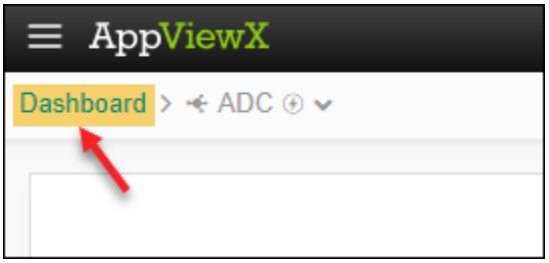
## Dashboard Tasks

- Rename a Dashboard
- Switch Between Dashboards
- Change the Settings for a Dashboard
- Delete a Dashboard

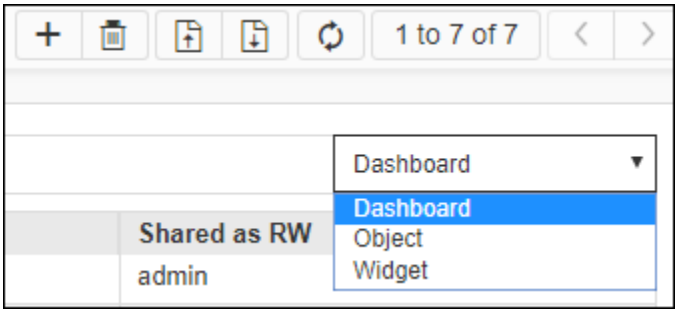
## Search for a Dashboard, Object, or Widget

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

1. Click ☰ and select **Dashboard**.
2. Click **Dashboard** in the breadcrumbs trails at the top of the screen to go to the top-level Dashboard screen or click ☰ in the Command bar.

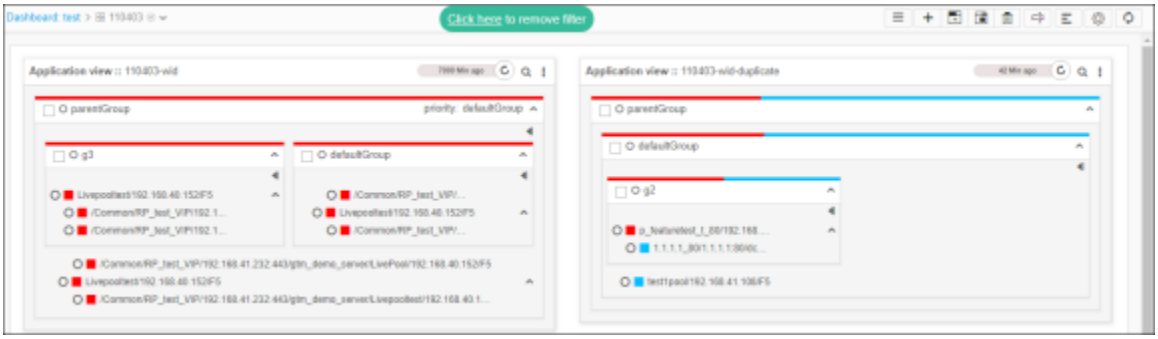



3. On the Dashboard screen that appears, enter the word or phrase you want to search by in the Search field.
4. Click the dropdown list at the right of the Search field and select the one you want to search for: Dashboard, Object, or Widget.




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`.

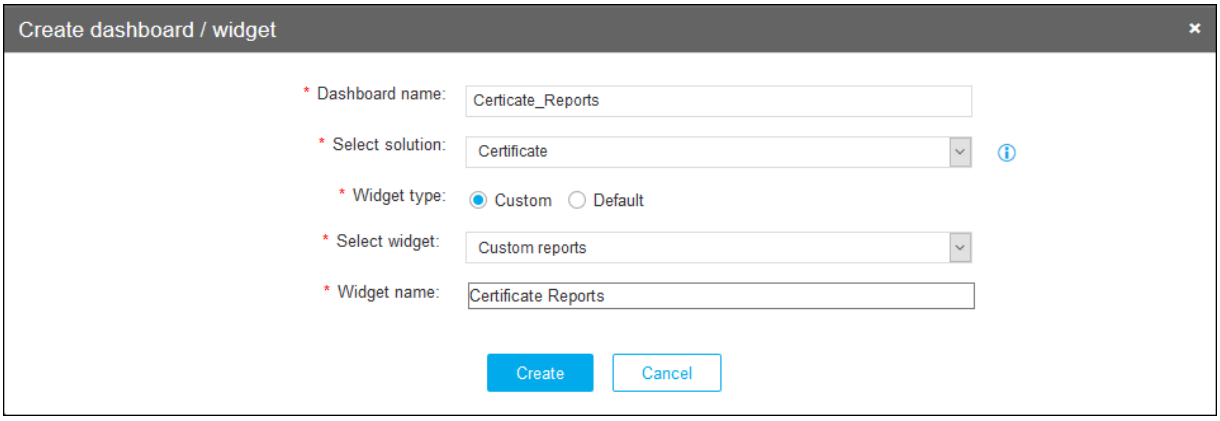


## Create a Dashboard

To create a dashboard:

1. Click ☰ and select **Dashboard**.
2. If this is the first dashboard you are creating in the system, click **Create Dashboard** in the center of the screen. If you have already created at least one dashboard, click + on the top-right.
3. In the **Create Dashboard / widget** pop up window, enter a name for the new dashboard.

> **Note:** The name cannot have 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. (Applicable only for **ADC solution**) 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, 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**.
   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.

## 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. Click  and select Dashboard.
2. After making necessary changes in the dashboard, click  in the Command bar.
   A pop-up message appears at the top of the dashboard: "Dashboard saved successfully."

## Share a Dashboard

To share a dashboard, complete the following steps:

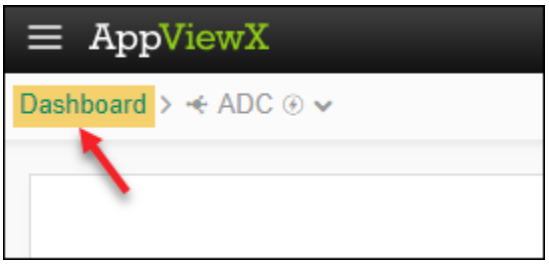
1. Click  and select Dashboard.
2. If you have more than one dashboard, in the dashboard table, click the name of the one you want to share.

3. When the dashboard opens, click  in the Command bar at the top of the screen. The Share screen appears.
4. Begin the assignment process by clicking R.
   Each role you assign next will have read-only permissions within the dashboard.
5. In the **Roles** field, click » beside each role you want to share the dashboard with on a read-only basis.
6. Click R/W.
   Each role you assign next will have read/write permissions within the dashboard.
7. In the **Roles** field, click » beside each role you want to share the dashboard with on a read/write basis.
8. Click **Share**.

## Export a Dashboard

To export a dashboard from AppViewX, complete the following steps:

1. Click  and select Dashboard.
2. Go to the top-level of the Dashboard module by clicking the Dashboard link in the breadcrumb field or click  in the Command bar.



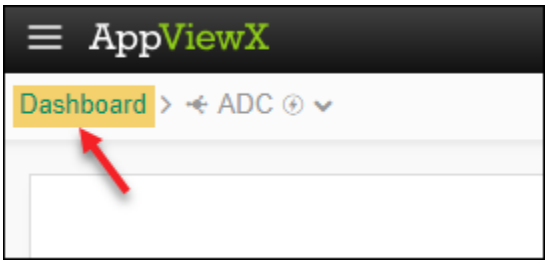

3. In the dashboard table, select the checkbox beside the dashboard you want to export.
4. Click  in the Command bar at the top of the screen.
5. On the **Export Dashboard** screen that pops up, select one of the following radio buttons:
   - Report (.csv) - Select this option if you want to view the 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**.

## 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. Click and select Dashboard.
2. Go to the top-level of the Dashboard module by clicking the Dashboard link in the breadcrumb field or click in the Command bar.




3. Click 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**.
   The import function then checks to make sure the imported file and file name are valid.


6. 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 **Submit**.
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

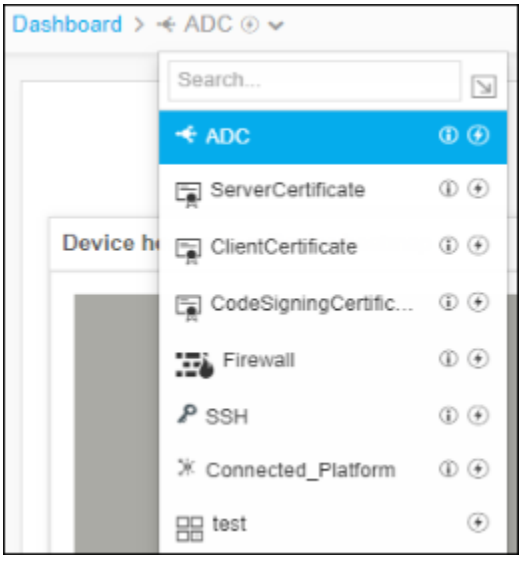
To rename a dashboard, complete the following steps:

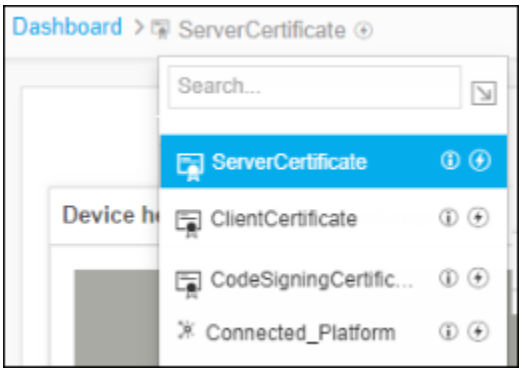
1. Click and select Dashboard.
2. If you have more than one dashboard, in the dashboard list, click the name of the one you want to rename.
3. When the dashboard opens, click in the Command bar at the top of the screen.
4. On the Rename dashboard screen that pops up, enter a new name for the dashboard.
5. Click **Update** to finish.

## Switch Between Dashboards

To switch from one dashboard to another, complete the following steps:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click on the current dashboard name.
3. In the dropdown list that appears, click the name of the dashboard you want to switch to.






You can also click in the Command Bar and click the name of the dashboard you want to switch to.

## Change the Settings for a Dashboard

To change the settings for a dashboard, complete the following steps:

1. Click icon and select Dashboard.
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 .
   A dropdown menu appears, listing the settings you can change:
   - If the **Refresh on load** setting is enabled, each time the dashboard loads, it displays the latest data in the system.
   - If the **Collapse group** setting is enabled, each time the dashboard loads, all groups within widgets on the dashboard display in a collapsed state by default.
   - If the **Keep alive** setting is enabled, the dashboard expiry function is disabled, allowing users to monitor all objects on the dashboard without interruptions caused by session time outs.
   - If the **Show only active** setting is enabled, the objects of an active device are displayed in run time. This functionality is applicable only for Application View widgets.

   **Note:** shows a Disabled setting and shows an Enabled setting.
4. To change a setting, click the corresponding icon and the opposite setting appears.

## Delete a Dashboard

To delete a dashboard, complete the following steps:

1. Click  and select Dashboard.
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  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.

## Widget Tasks

- Application View Widget Actions
- Configure an Application View Widget
- Configure a Traffic Statistics Widget
- Configure a Script Execution Widget
- Configure a Traffic Grid Widget
- Configure a Class Management Widget
- Configure a Heatmap Widget
- View the Different Statuses and States for a Widget
- Filter Objects in an Application Widget
- Sort the Objects in an Application Widget
- Enable or Disable Objects Displayed in a Widget
- Perform Bulk Actions on Objects in a Widget
- Force LTM Servers Offline Within a Widget
- Copy a Widget to Another Dashboard
- Move a Widget to Another Dashboard
- Delete a Widget
- Download the Contents of an Application View Widget
- Delete a Group, Object, or Action from an Application View Widget
- Search for an Object in an Application View Widget
- View Details About an Object in an Application View Widget
- Change the Percentage Values Within a Traffic Grid Widget

## Application View Widget Actions

The following actions can be performed on an Application View widget by right-clicking the widget and accessing the Actions menu:

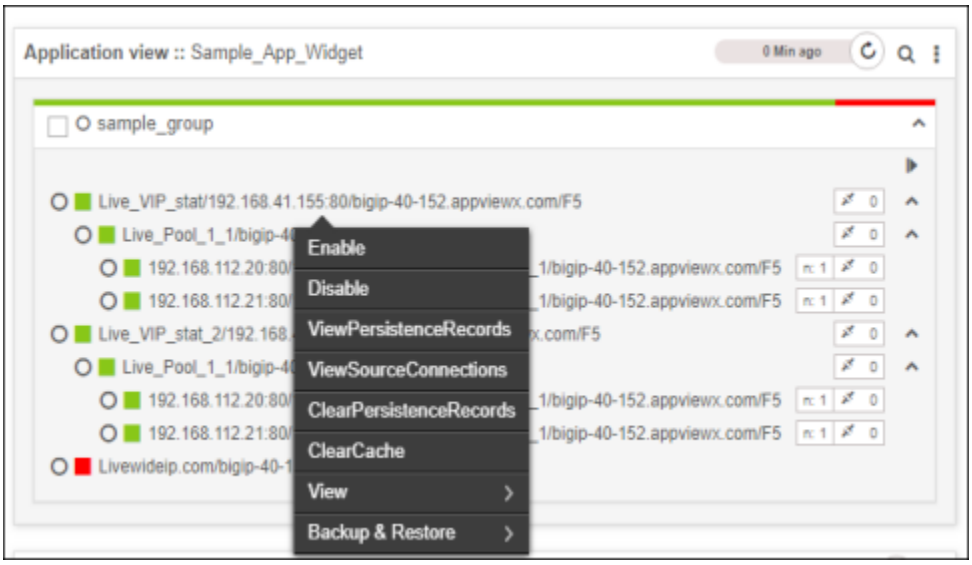
- Enable - Enable an object
- Disable - Disable an object and terminate all active connections
- **Enable/Disable all** - Enable or disable all objects in the widget at the same time
- Enable/Disable persistence (F5 devices only) - Turn on or off the tracking and storing of session data, which is used to ensure that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.
- 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
- ForceDown (F5 devices only) - Force a shutdown of the object
- Forcedown all
- (F5 devices only) - Force a shutdown of all F5 devices in the widget at the same time
- FD clear active connections (F5 devices only) - Clear active connections to the object
- **Clear RAM cache** - Clear the RAM cache of an object
- Clear persistence records (F5 devices only) - Clear persistence records for VIP and pools
- **Set Highest Priority** - Set the priority for the pools of a wide IP.
- **View**
  - **View graph** - View the timeline statistics of the object
  - **View config** - View the configuration code for the object in a popup screen
  - **View log** - View the log history of the object
  - **View alerts** - View any alerts related to the object
  - **View topology** - Open the topological view that contains the object
- **Backup device** - Create a backup of the device associated with the object
- **Restore device** - Restore object configuration to a previous state

## Configure an Application View Widget

An Application View widget allows users to group the service objects of a single application. The widget allows the user to manage and monitor the applications by displaying the health of their objects and the number of current connections that the services are receiving.

To configure an Application view widget on your dashboard, complete the following steps:

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  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 name for the widget.
6. Click **Create**.
   The Settings screen for the Application view widget opens, displaying an empty **DefaultGroup** where the user can add the objects.
7. Modify the widget name, group name, and add a description by clicking the corresponding fields.
   It will then becomes a text-entry field that allows you to make changes.
8. Click the **Add/Modify Objects** button to add the objects at the group level.
9. Select the vendor from the dropdown list.
10. 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.
11. In the Device Name field, select the device name whose objects you want to add to in the widget.
12. 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.
13. 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.
14. Select the checkbox beside the object name and click **Add** to add the objects to the group.
    - The **Actions** and **Attributes** corresponding to objects added will be automatically listed in their respective sections.
    - By default, access to the actions and attributes apply to all objects within that group. You can customize these permissions manually by selecting or deselecting permissions for individual objects. 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.
15. 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.
16. Click  or  to hide or view the full list of attributes you created for a group.
17. When you have finished, click **Save**.
    The dashboard screen reappears, displaying the widget you just created.




18. To create a new group, complete the following steps:
    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**.

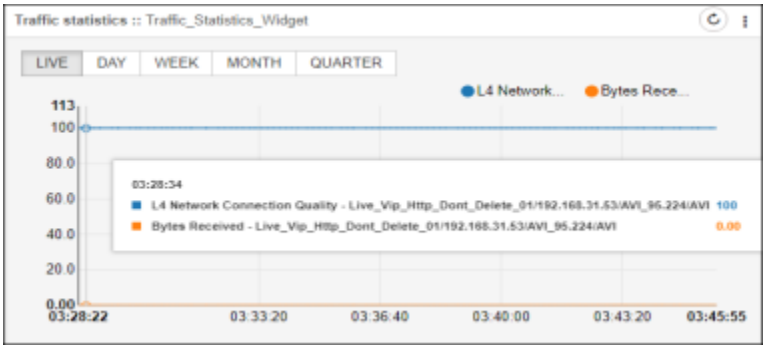
## Configure a Traffic Statistics Widget

A Traffic statistics widget displays a chart showing live and historic performance statistics for individual device objects including the number of requests being received, the loads on each of the load balancers, and peak request times.

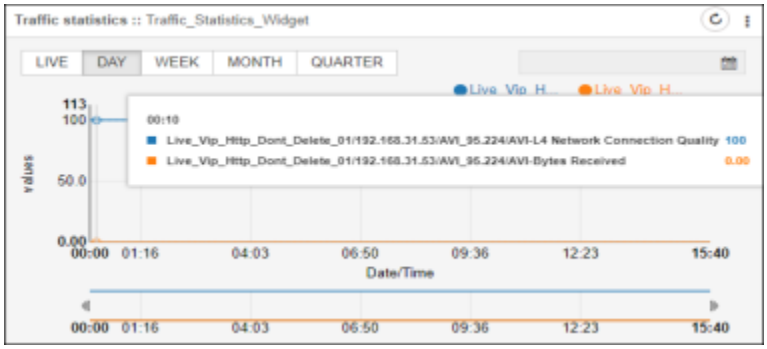
To configure a Traffic statistics widget on your dashboard, complete the following steps:

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  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.
    The dashboard screen reappears, displaying the widget (Live performance statistics) you just created.



- 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 Management** section in the ADC Settings topic of this guide.




- Click on Day/Week/Month/Quarter tab within the widget to view the historic performance statistics.

## Configure a Script Execution 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 perform 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.

To configure a Script execution widget on your dashboard, complete the following steps:

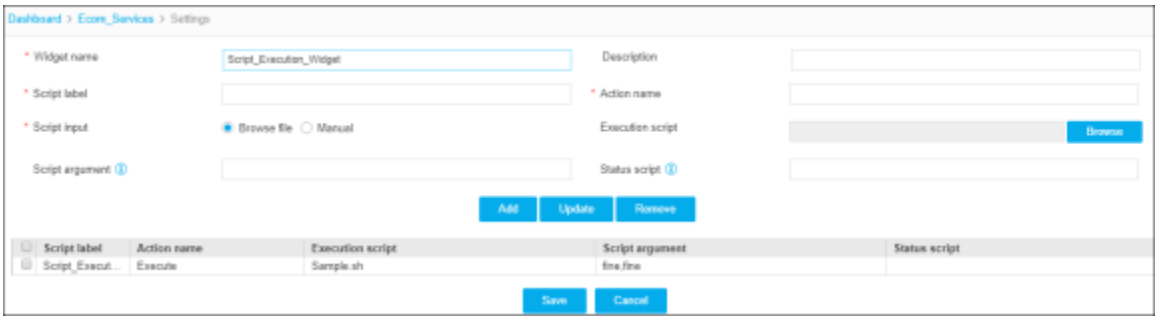
1. If you are creating a Script execution widget as part of creating a new dashboard, complete the steps in the Create a Dashboard topic above, then jump to Step 5 below. If you are creating a Script execution widget for an existing dashboard, click  in the Command bar of the dashboard.
2. On the Create 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:

a. 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**.

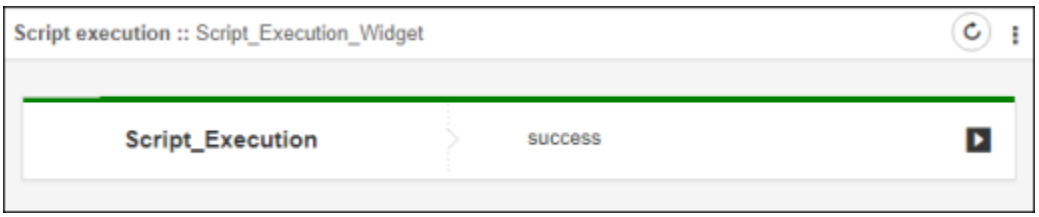
b. If *Manual* is selected in Step 8, enter the full path of the script. These scripts will need manual intervention to execute.

10. In the **Script argument** field, enter any information for the script with space as delimiters.
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. When the widget is viewed on the dashboard, each script appears with a ▶ beside it.




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 |

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

16. 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.

When it finishes, a popup screen appears listing the script execution logs, as shown in the following example.


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

## Configure a Traffic Grid Widget

A Traffic grid widget allows users to 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.

To configure a Traffic grid widget on your dashboard, complete the following steps:

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  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 an application you want to monitor traffic for.
6. Click  to add the application to the list.
7. Enter the names of a data center you want to configure traffic flows for.

8. Click + 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**.

    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.


11. Click ⚙ icon inside each Application/Datacenter cell of the grid to configure it.

    The Settings screen appears, with the Availability status tab displayed by default.
12. Select the vendor whose object you want to monitor availability for in each data center.
13. 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.
14. Click **Add**.
15. Repeat steps 15-16 for any other objects you want to monitor.
16. When you have finished adding all of the object types whose availability you want to monitor, click Save.
17. Click the **Traffic Percentage** tab.
18. Select the vendor whose object you want to monitor traffic across all data centers.
19. 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.
20. In the Object type field, select the kind of object you are adding: **wideIp Pool**,wideIp PoolMember, or ItmPoolMember.
21. 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.
22. Repeat steps 23-24 for any other objects you want to monitor.

23. When you have finished adding all of the object types whose traffic percentages you want to monitor, click Save.
24. Click the Statistics tab.
25. In the Display name field, enter the text you want to pop up when a user hovers over the icon within a table cell of the widget.


> **Note:** Only 10 characters can be entered in the field, so the name must be brief, but descriptive.

26. In the Vendor field, select the vendor whose object you want to generate statistics across all data centers.
27. In the Device state field, select whether you want to generate statistics for a device that has a status of Active, Standby, or All.
28. In the Object type field, select the kind of object you are adding: wideIp PoolMember or ItmPoolMember.
29. 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.
30. Click **Add**.
31. Repeat steps 32-33 for any other objects you want to generate statistics for.
32. Click **Save**.
33. Click the Rules tab if you want to create rules that govern traffic percentages for the widget.
34. In the Rule type field, select one of the following options:

- 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 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  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.

35. When you are finished creating rules for the widget, click Save.

> **Note:** 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.

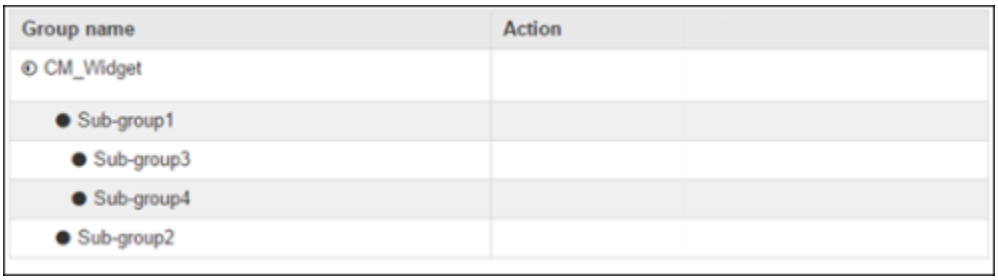
## Configure a Class Management Widget

A Class management widget allows users 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.

To configure a Class management widget on your dashboard, complete the following steps:

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  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 name for the widget.
4. Click Create.
5. On the Settings screen, enter a name for the widget or leave the default value as is.
6. Leave the Select task field set to CreateGroup.
   The Group field automatically uses the widget name as the default group.
7. Enter a name for the group.
8. Click Add to add the group to the widget.
9. (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.

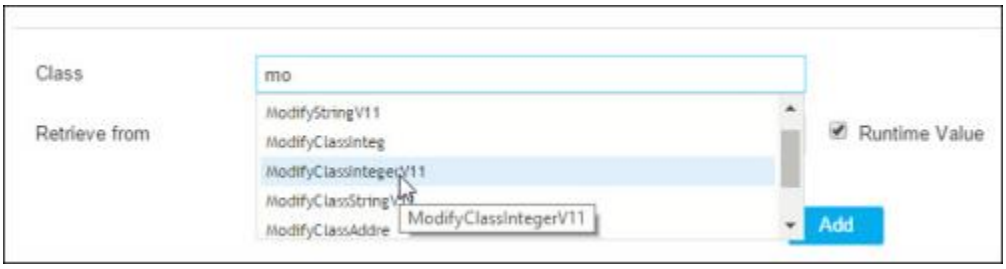
10. (Optional) If you want to create a sub-group of a sub-group, select the sub-group in the Group dropdown list, then enter the sub-sub-group name in the Name field before clicking Add.
    In the example below, CM_Widget is the group, Sub-group1 and Sub-group2 are created as sub-groups of CM_Widget, and Sub-group3 and Sub-group4 are created as sub-groups of Sub-group1.




11. After you have finished creating groups and sub-groups, select CreateAction from the Select task dropdown menu.
    The screen refreshes to display new fields on the screen.
12. In the Actions field, select one of the following options:

    - View Class - This option gives users the ability to see the details of a class without being able to make any changes
    - Modify Class - This option gives users the ability to view and change the details of a class
    - In the Group field, select the group you are creating the action for.
    - In the Name field, give the action a name that clearly identifies what action the user can take.


13. In the Class field, start typing the name of the class that you are creating a *view* or *modify* action for.



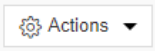

As you start to type, all classes that match the characters you have entered so far appear in a list.

14. Select the class you want to add.

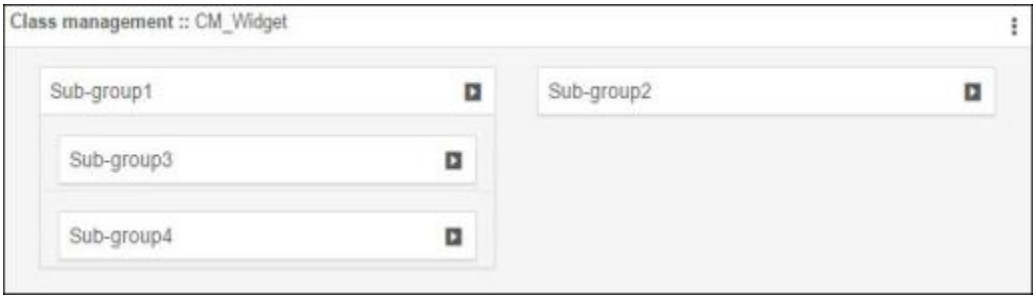
    The Retrieve from field populates automatically with the location of the class that you selected in Step 15.

15. If you are creating a View Class action, click Add to add the class to the group. If you are creating a Modify Class action, use the new fields that appear on the screen to do the following:
    - Add or remove values from the selected class using » in the Available Values field and « in the Selected Values field.
    - Add or remove devices from the selected class using » in the Available Values field and « in the Selected Values field.
    - Repeat steps 12-16 for each additional action you want to add to the group.
    - Click Save when you are done.

    The group and all sub-groups you just created appear in a hierarchical structure within the widget.

16. Click 

to access the list of available actions for the corresponding group or sub-group.




## Configure a Heatmap Widget

A Heatmap widget allows users to view statistics for managed, failed, and unresolved devices or device groups relating to the following parameters:

- **CPU Utilization** - Total usage of CPU in percentage along with the unused CPU limit
- **Memory Utilization** - Used memory space in percentage
- **Bandwidth Utilization** - Total bandwidth limit along with the used bandwidth percentage

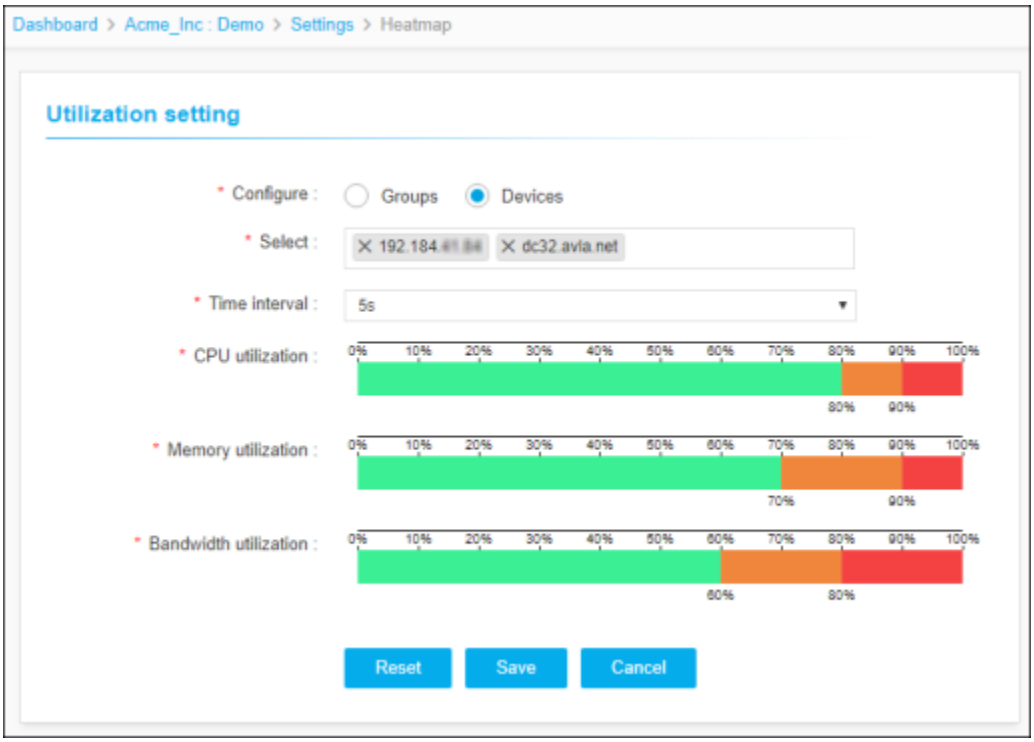
- **Device Information** - Statistical information including expiry date, vendor, version, and uptime
- **Alarms** - All alerts corresponding to each device included in the heatmap
- **Logs** - All logs corresponding to each device included in the heatmap
- **Graph** - Displays the current connections for each device included in the heatmap
- **iHealth reports** (F5 devices only)

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

To configure a Heatmap widget on your dashboard, complete the following steps:

1. If you are creating a Heatmap 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 Heatmap widget for an existing dashboard, click  in the Command bar of the dashboard.
2. On the Create widget screen that pops up, select Custom as the widget type.
3. Enter a name for the widget.
4. In the Basic charts field of the Settings screen, click the Heatmap option.
5. In the Filter query field, click the groups you want to include in the heatmap.
6. Click Next.
   A Heatmap widget configuration screen appears.




7. In the **Configure** field, select the **Groups** or **Devices** radio button depending on whether you want the heatmap to show data for device groups or individual devices.
8. In the **Select** field, click the dropdown arrow and select each of the groups or devices you want to include in the heatmap.
9. In the Time interval field, select the frequency that you want the system to check the utilization levels of the devices or groups you selected in Step 7.
10. In the **CPU Utilization** field, click and drag the sliders to define the safe, warning, and critical value limits for device CPU.
11. In the **Memory Utilization** field, click and drag the sliders to define the safe, warning, and critical value limits for device memory.
12. In the **Bandwidth Utilization** field, click and drag the sliders to define the safe, warning, and critical limits for device bandwidth.
13. When you are done configuring the heatmap settings, click **Save**.
    The heatmap widget then displays on the dashboard, with separate, color-coded blocks representing the following for each of the devices or groups you selected.
    • Green - CPU, memory, or bandwidth usage within safe limits.
    • Orange - CPU, memory, or bandwidth usage within warning limits
    • Red - CPU, memory, or bandwidth usage within critical limits
    • Gray - Missing or no information for the related group or device

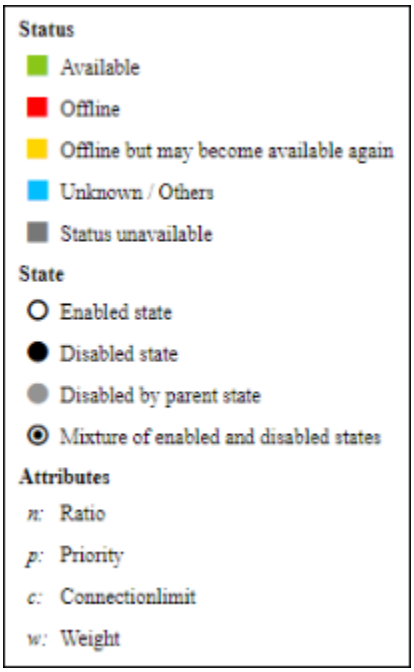

On hovering your cursor over a device or group, the following information appears in a popup tooltip:

- Current CPU utilization for the device/group
- Current bandwidth utilization for the device/group
- Current memory utilization for the device/group

## 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:

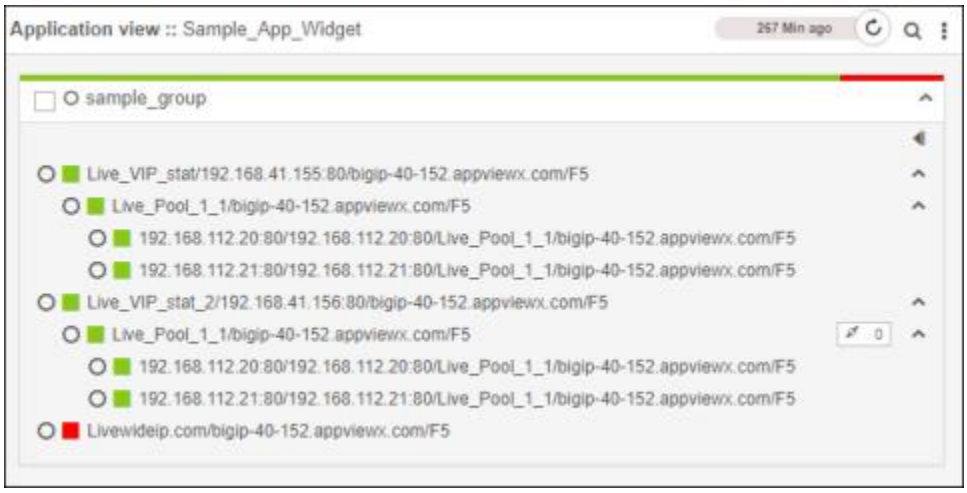
1. Click ☰ and select Dashboard.
2. Select a dashboard that has an Application view or Traffic grid widget.
3. Click ⋮ and select ■ in the Command bar at the top of the widget.
   A legend appears, listing each of the possible widget statuses and states. For Application view widgets, there are five possible statuses and four possible states, as shown below.




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


- 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.

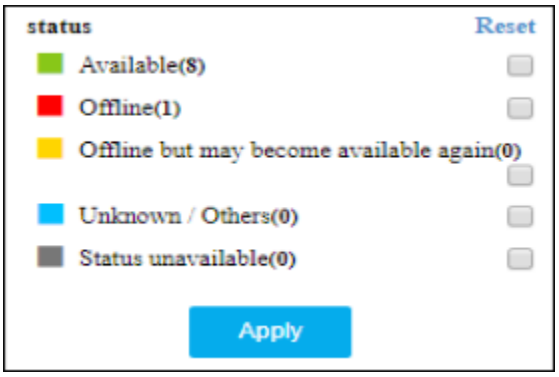



- The temperature bar, which is the colored bar at the top of each group or object name, displays the overall status of all components within the widget. In the example above, note that the virtual server group shows a solid green temperature bar because all components under it are Available, whereas 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.

## Filter Objects in an Application Widget

To filter the objects displayed in an application widget based on their status, complete the following steps:

1. Click and select **Dashboard**.
2. If you have more than one dashboard, in the dashboard list, click the name of the one containing the Application view widget.
3. Click and select in the Command bar at the top of the widget.
4. In the **Status** field that appears, select the checkboxes beside each status you want to have displayed in the widget.




5. Click the **Apply** button to initiate the filtering process.
   The widget then refreshes and displays only objects having one of the statuses you selected.
6. To unfilter the widget contents, click the filter icon again and then click the Reset link in the **Status** field. Then click outside the field to initiate the filter removal process.

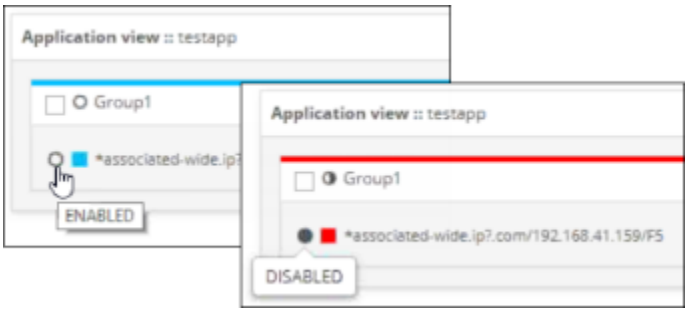
## Sort the Objects in an Application Widget

To sort the objects displayed in an application widget based on the ascending or descending order, complete the following steps:

1. Click and select Dashboard.
2. If you have more than one dashboard, in the dashboard list, click the name of the one containing the Application view widget.
3. Click and select **Ascending**/ **Descending** in the Command bar at the top of the widget.
   The objects will be arranged and displayed in the corresponding order.

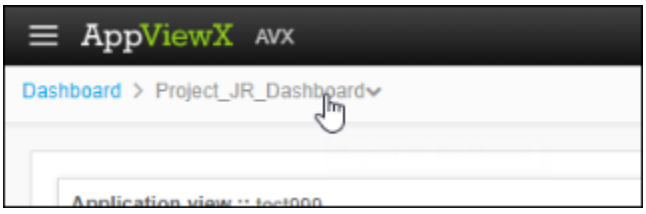
## Enable or Disable Objects Displayed in a Widget

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.

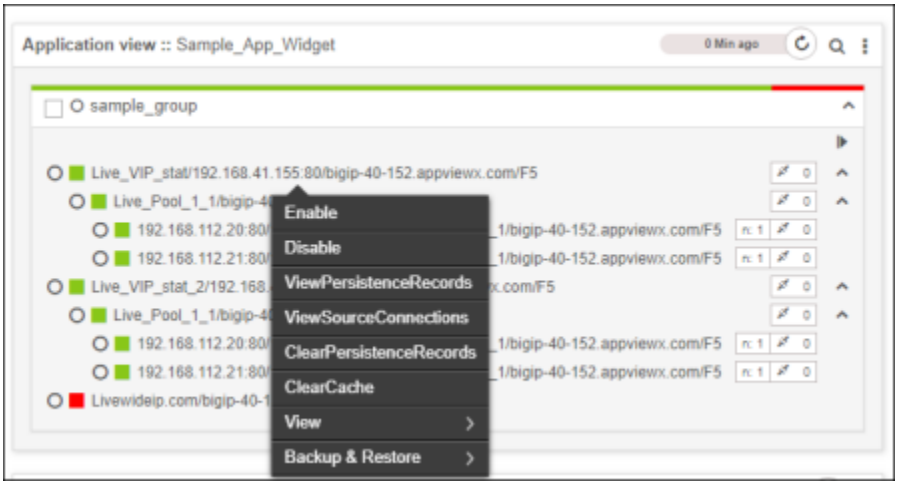



To enable or disable objects displayed in a widget, complete the following steps:

1. Click .
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.



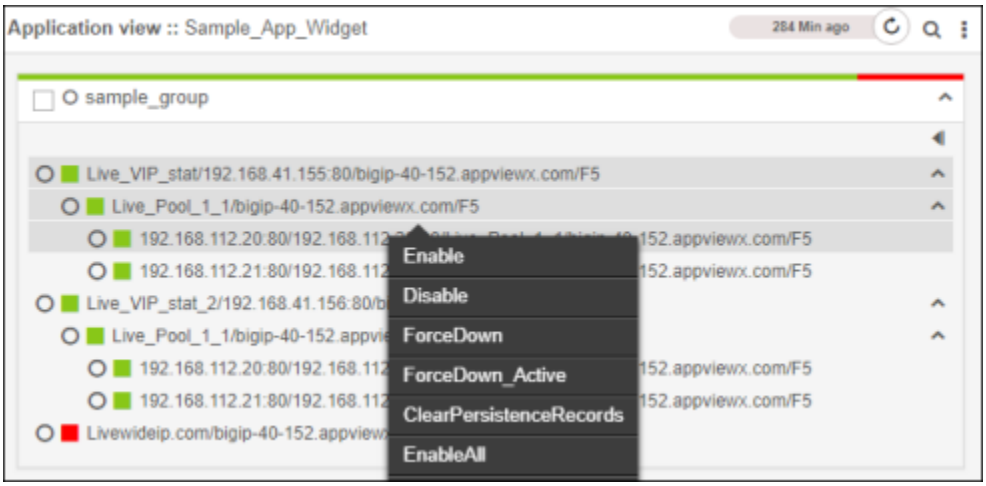

7. On the Confirmation screen that pops up, enter comments relating to the enable or disable action, then click **Yes**.
8. Click in the widget Command bar to see the updated view of the widget.

## 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, complete the following steps:

1. Click .
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 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. Click .
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 in the widget Command bar to see the updated view of the widget.

## Copy a Widget to Another Dashboard

To copy a widget to another dashboard, complete the following steps:

1. Click and select **Dashboard**.
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 and select 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 to.
5. Click **Copy to Finish**.

## Move a Widget to Another Dashboard

To move a widget to another dashboard, complete the following steps:

1. Click select **Dashboard**.
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 and select 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. Click and select **Dashboard**.
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 and select in the Command bar of the widget.
4. On the confirmation screen that pops up, click **Yes**.
   The dashboard refreshes and no longer displays the widget.

## Download the Contents of an Application View Widget

The download feature is only available for Application view widgets.

To download the contents of an Application view widget to a CSV file, complete the following steps:

1. Click and select **Dashboard**.
2. If you have more than one dashboard, in the dashboard list, click the name of the one containing the Application view widget whose contents you want to download.
3. Click and in the Command bar at the top of the widget.
4. On the screen that opens, select the location where you want the CSV file to go, then click **Save**.

## Delete a Group, Object, or Action from an Application View Widget

To delete a group, object, or action from an Application view widget, complete the following steps:

1. Click and select Dashboard.
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 and select in the Command bar at the top of the widget.
4. On the Settings screen that appears, the Groups tab is displayed by default.(Optional) Click one of the groups or subgroups in the list on the screen, then click **Delete**.
5. On the popup screen that appears, click Yes to confirm the deletion.

> **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 clickable.

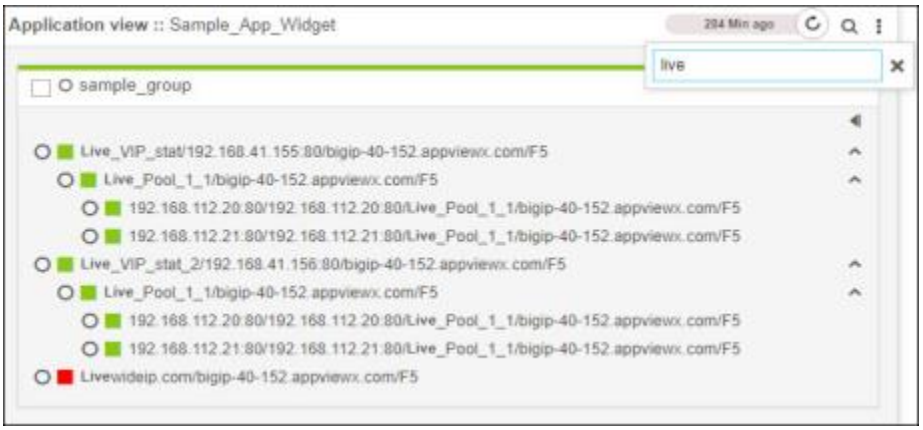
6. Click **Save**.
7. Repeat steps 4-6 for each of the other groups you want to delete.
8. (Optional) Click the **Objects** tab.
9. In the Group Name field, select the first group that you want to remove objects from in the widget.
10. In the Added Objects field, click « beside each object you want to remove from the group.
11. Click **Save**.
12. Repeat steps 8-11 for any other groups that you want to delete objects from in the widget.
13. (Optional) Click the **Actions** tab.
14. In the Group name field, select the group you want to delete actions from.
15. In the Action field, select the first action you want to delete from the group.
    The Delete button becomes clickable.
16. Click **Delete**.
17. On the screen that pops up, click Yes to confirm that you want to delete the action.
18. Click **Save**.

19. Repeat the process to remove any other actions you want from the group.
20. When you have finished with the first group, repeat steps 14-20 for any other groups that you want to remove actions from.

## Search for an Object in an Application View Widget

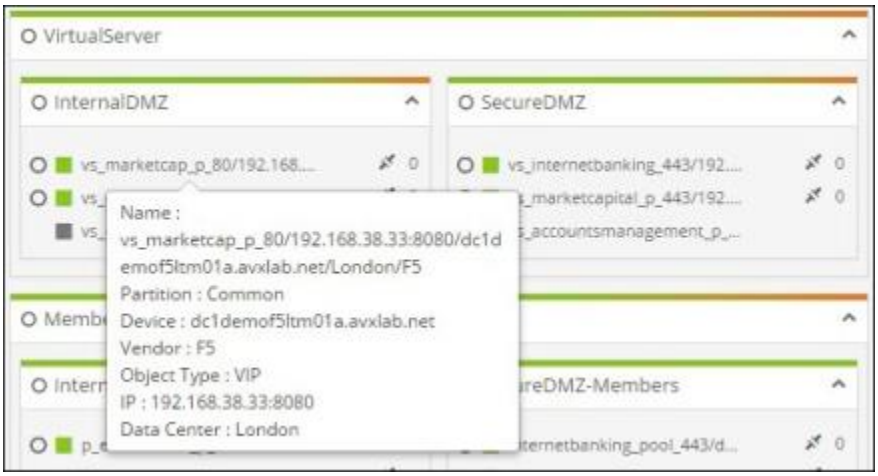
To search for an object in an Application view widget, complete the following steps:

1. Click ☰ and select Dashboard.
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 🔍.
4. In the search field that pops up, begin entering the name or number of the object you want to find. 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.




## View Details About an Object in an Application View Widget

To view details about any object in an Application view widget, hover your cursor over the object name and a details screen pops up.




## 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.
   The cell then becomes a text-entry field, as shown in the bottom-right cell in the image below.


3. Enter the new percentage in the text field.
4. Click ✔ to save your changes.
5. Repeat the process for each of the other data centers, ensuring that the total equals 100%.

> **Note:** For an explanation of the different colors and symbols displayed in the cells, refer to View the Different Statuses and States for a Widget.

# Chapter 3: Control Center

- Create a WAF Policy
- Download a WAF Policy
- Compare WAF Policies
- Modify a WAF Policy
- Delete a WAF Policy
- Access the Actions Menu for Objects on the ADC Search Results and Topology Screens
- Access the Actions Menu for Objects Within Certificate Topologies
- View Complete Details of a Certificate
- Access the Actions Menu for Rules on the Firewall Search Results Screen
- Access the Actions Menu for Keys Within SSH Holistic View

## Control Center Module

The Control Center module is a centralized object repository that allows you to search for and then monitor and manage the objects, applications, and certificates that exist within the AppViewX platform.

In order to use the Control Center module, the following prerequisites must be met:

- Each device you want to control must be a managed entity in AppViewX.
- You must have been assigned to a role and resource that has the appropriatedevice/object levelaccess to thedevices,certificates, and policies that you want to control. However, for the orphan and secondary objects, global access must have been provided.

You can perform a wide range of actions directly from the Control Center:

- Run a search
- Create a bookmark
- View basic details of search results
- View additional details of search results
- View the Certificate Search Results
- Filter ADC search results
- Export ADC and SSH search results

- View orphan objects
- View timeline statistics for an object
- View object configuration details
- Compare ADC objects
- View nested group for a firewall rule
- View WAF threat protection settings
- Compare WAF policies
- Work with ADC objects through the search results and topology screens
- Work with Certificate topologies
- View complete details of a certificate
- Work with SSH topology screen

# Run a Search Within the Control Center

To run a search within the Control Center:

1. Click  .
2. From the navigation menu, select Control Center.

   The Control center opens with the search screen displayed by default. There are different ways you can search on this screen:

   - Text entry
   - Frequent search links
   - Regex
   - Search keys

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

## Search Using Free Text Entries

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

- Case insensitive keyword and string matching.
- Exact match search strings through the use of double quotation marks around search terms.
- Boolean AND and OR operators:
  - AND search results contain both terms that existed in the search query.For example, a search for AppViewX AND firewall returns only those objects whose descriptions contain both AppViewX and firewall.
  - OR search results contain one or both terms that existed in the search query.A search for AppViewX OR firewall returns all objects whose descriptions contain AppViewX, firewall, or both AppViewX and firewall.
  - If a Boolean AND operator and an OR operator exist in the same search string, the AND operator is executed first by 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.
- (Only for Firewall) Exclusion of specific words, terms, or character strings from search results through the use of the negate symbol followed by the term to be excluded enclosed within quotation marks. For example, entering -"POL31" and action: allow returns all rules with their action set to allow, except those that belong to POL31.
- (Only for Firewall) Comprehensive IP address searches using the source IP or destination IP criteria. The results list includes all overlapping subnets or IP ranges. For example, a search for 192.168.2.254 would also display rules containing a subnet such as 192.168.2.0/24 or an IP range such as 192.168.2.0-192.168.2.255.

## Search Using Frequent Search Links

The Control center 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  button next to the search bar and select **Frequent Searches** to view a list of frequent searches.

## 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 its hierarchy are displayed in their respective tabs.
- **(object name).***- The objects that start with the name you entered in the search field are fetched and displayed.
- **(certificate name)***- The certificates that start with the name you entered in the search field are fetched and displayed.
- The search results that are matched with the text entered will be highlighted.

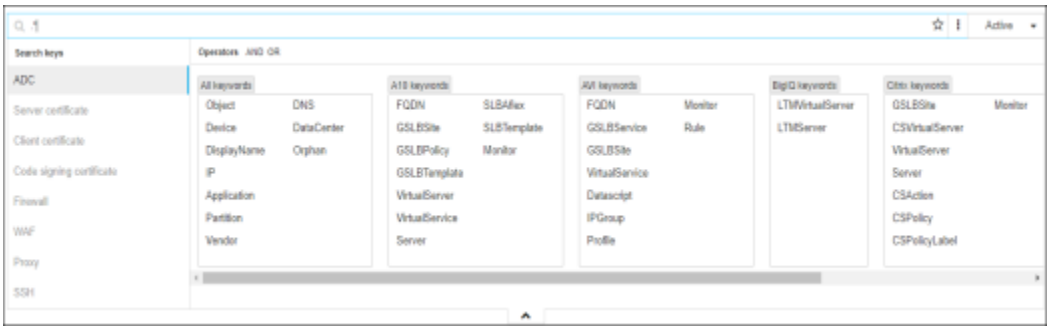
## Search Using Search Keys

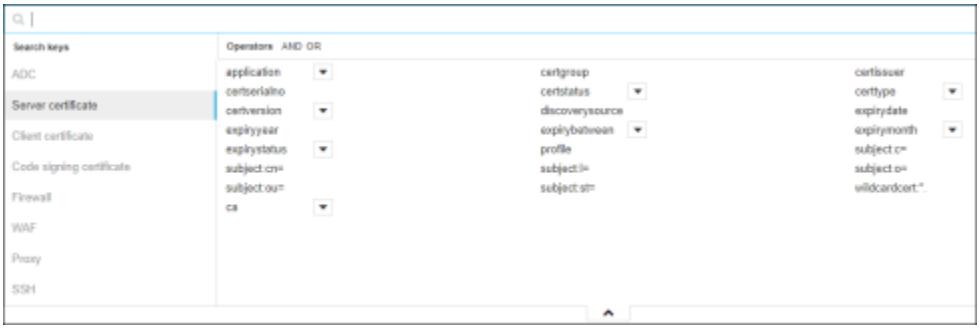
Search keys are predefined metadata types, sorted by object type,that you can use to create highly targeted search queries. To create a search key query, complete the following steps:

For the sample, search queries used for ADC objects and an explanation for the ADC, Certificate, Firewall, and WAF, Proxy, and SSH search keys, refer to the callout boxes at the end of this topic.

| ADC Search Queries | |
|---|---|
| The following are the various sample search queries that are used to fetch the ADC object details: | |
| virtual server:* AND device: F5_v11 | The list of virtual servers available in the specific device |
| Rule:* AND device: F5_v11 | The iRule available in the specific device |
| device: F5_v11 AND virtual server:* AND IP:192.168.96.101 | The list of virtual servers in the specific device that uses the IP address 192.168.96.101 are identified |
| object: Citrixv11 CSvirtualserver AND CSvirtualserver:* | The list of content switching virtual servers that have the object name you mentioned in the search query |
| object:server_123 AND IP:192.168.96.101 and device: F5_v11 | The list of objects in the specific device that has the object name and IP address you mentioned in the search query |

1. On the Search screen, click  at the bottom of the search field.
2. The field expands to display a list of search keys available for the ADC Certificate.





3. If you want to search for primary or secondary ADC objects, stay on this tab. Otherwise, click one of the other tabs. Click any of the metadata types in the list to add them to the search query.
4. 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."
5. (Optional) Click the AND and OR operators at the top of the Search keys field to create Boolean searches.
6. When you are finished creating the search query, click inside the search field, then click **Enter** on your keyboard to run the search.

| ADC Search Key Definitions | |
|---|---|
| The following are definitions for some of the less obvious search keys on the ADC search tab: | |
| aflex | An advanced scripting language for A10 Thunder and AX series |
| class | The class helps in listing the data group configured in F5 |
| policy label | The content switching policy label configuration |
| profile | The list of profiles associated with the primary objects of F5 and Citrix vendors |
| policy | The LTM policy of F5 device and content switching policy of Citrix device |

| Certificate Search Key Definitions | |
|---|---|
| The following are definitions for some of the less obvious search keys on the Certificate search tab: | |
| subject:c= | The country where the certificate was issued |
| subject:cn= | The common name of the certificate |
| subject:l= | The location where the certificate was issued |
| subject:o= | The organization that issued the certificate |
| subject:ou= | The organization unit issued the certificate |
| subject:st= | The state where the certificate was issued |

| Firewall Search Key Definitions | |
|---|---|
| The following are definitions for the search keys on the Firewall search tab: | |
| device | The target firewall device associated with the policy |
| source/ destination | The source or destination object associated with the policy or rule managed within the device |
| sourceip/ destinationip | The source or destination IP address associated with the policy or rule managed within the device |
| tsource/ tdestination | The translated source or destination object associated with the policy or rule managed within the device |
| tsourceip/ tdestinationip | The translated source or destination IP address associated with the policy or rule managed within the device |
| tservice | The translated service of a NAT rule associated with the policy managed within the device |

| WAF Search Key Definitions | |
|---|---|
| The following are definitions for the search keys on the WAF search tab: | |
| policy | The policies available within the device |
| service | The service associated with the policy managed within the device. For example, TCP-8080, UDP-5 |
| mode | Defines the mode of the policy |

| WAF Search Key Definitions | |
|---|---|
| source/ destination | The source or destination object associated with the policy or rule managed within the device |
| sourceip/ destinationip | The source or destination IP address associated with the policy or rule managed within the device |

| Proxy Search Key Definitions | |
|---|---|
| The following are definitions for some of the search keys on the Proxy search tab: | |
| policy | The policies available within the device |
| port | The port number of the device |
| action | The actions (such as allow, deny, reject, and so on) associated with the policy managed within the device |
| rule | The rules available within the device |
| sourcedomain/ destinationdomain | The source or destination domain name associated with the policy or rule managed within the device |

| SSH Search Key Definitions | |
|---|---|
| The following are definitions for some of the search keys on the SSH search tab: | |
| keyname | The name of the user-defined key pairs |
| IP address | The IP address associated with the SSH keys |
| keyfingerprint | The key with the matching key fingerprint search value (either with the current key fingerprint). A total number of 50 key fingerprints per key are saved in AppViewX |
| hostfingerprint | The host-associated to the key with the matching host fingerprint |
| createuser | The list of keys created by the user (key owner) |
| associateduser | The list of keys associated with the user (single or multiple users who are using the same keys) |

## Create a Bookmark

To create a bookmark for the ADC frequent search items:

1. Click and select Control Center .
2. Run a search.
3. On the search results screen, click next to the search bar.
4. Click to create a bookmark folder.
5. Click 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**.
8. You can delete the bookmark by clicking the **Remove** button.
   A pop-up message will be displayed at the top of the screen, **Bookmark(s) deleted successfully**.

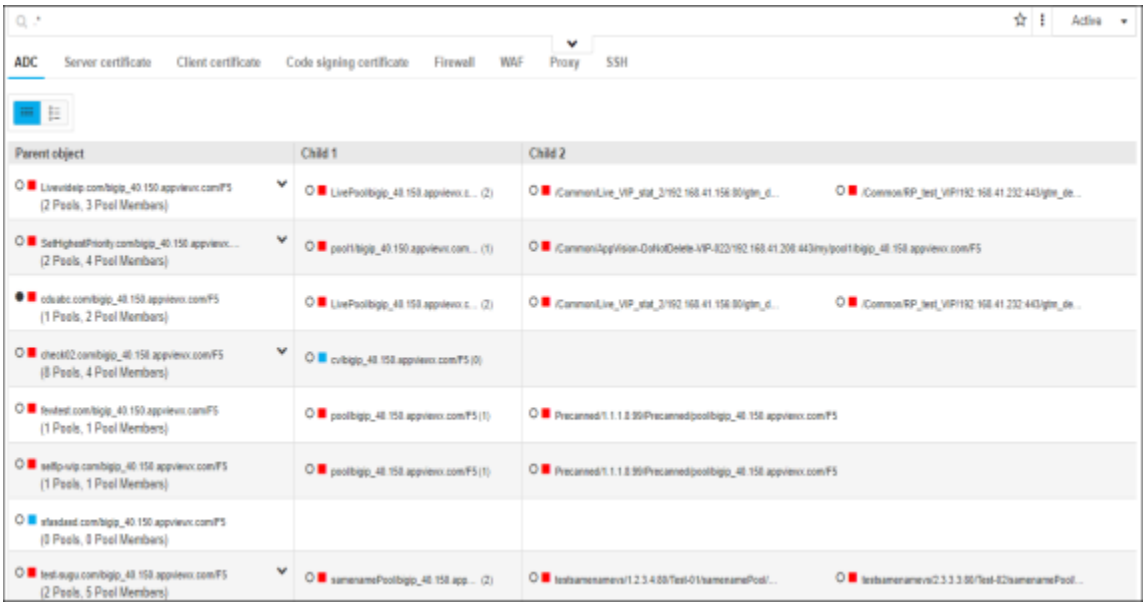
# View Basic Details of ADC Search Results

Control Center module 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.

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

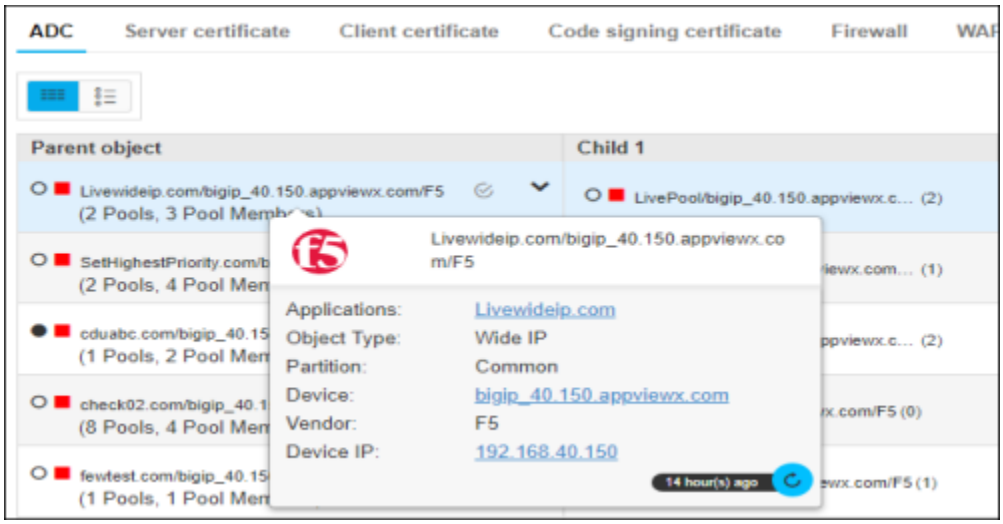
## Application View

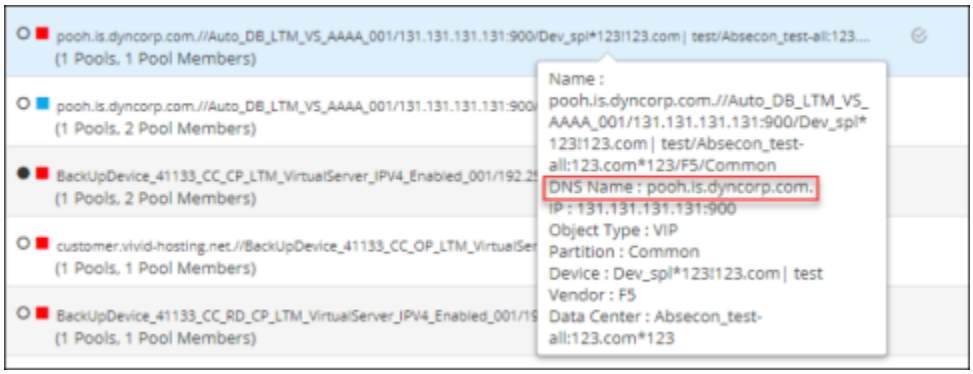
This is the default search result landing page. The parent objects are listed in the left column and related first-level children and second-level children appearing in columns to the right.




Each object has a series of symbols that appear before its name:

- Circles
  - 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
  - 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
- 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.

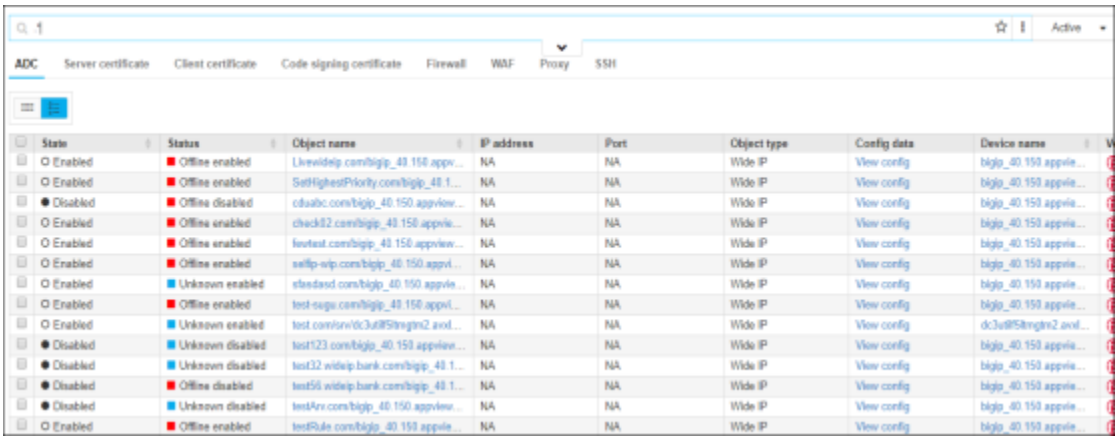



- The DNS name of an object (applicable only for F5 device objects) will be displayed in the pop-up box only if DNS is configured during AppViewX installation.

## 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). You must click  to switch from the Application view.

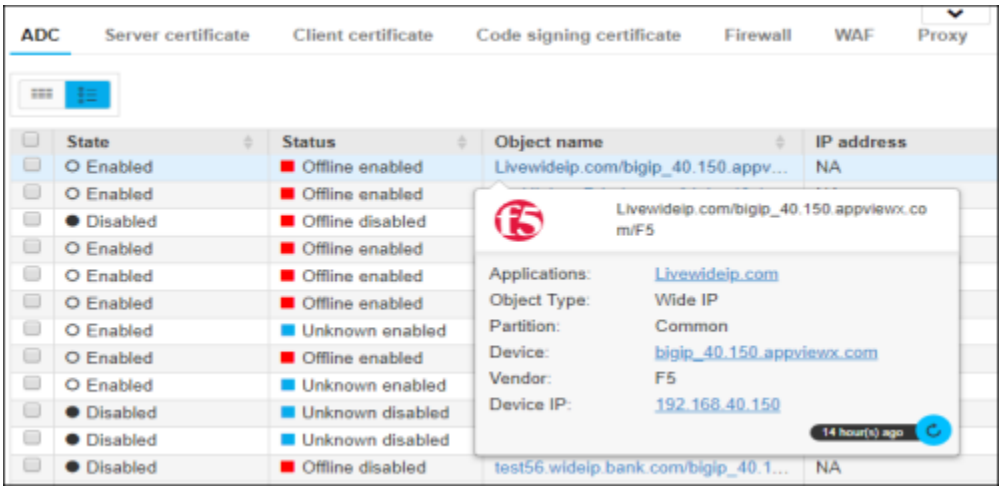



You can customize the columns as required and save the changes. This will render the columns every time the user logs in. For more details on how to customize the columns, refer to the Modify the Layout of a Screen section of this guide.

- State and Status of the object
- Name of the device and object based on how it is configured
- The IP address and port number of the object
- Type of object
- Configuration of the object
- Name of the Vendor
- IP/FQDN of the device
- Live connection count of the objects. You can refresh a specific record to view the updated value
- Partition/tenant/context of the object
- DNS resolution of the object

The following columns are displayed when you search for an object:

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




For instructions on how to view *complete* details of a search result, refer to View Additional Details for Search Results.

## Tooltip Information

The amount of information displayed in the popup varies depending on the type of object you hover over. This actionable tooltip of an object displays the Application names, Partition, Device, Vendor, and Device IP to which that particular object has been associated with.

Upon clicking the link, the following occurs:

- **Application** - A detailed Inframap will be displayed.
- **Device** - The device details screen that allows the user to make whatever modifications you want to the device details and then, click **Save**.
- **Device IP** - A device log in page will be displayed.

You can also refresh the data that appears on a tooltip by clicking .

# View Additional Details of Search Results

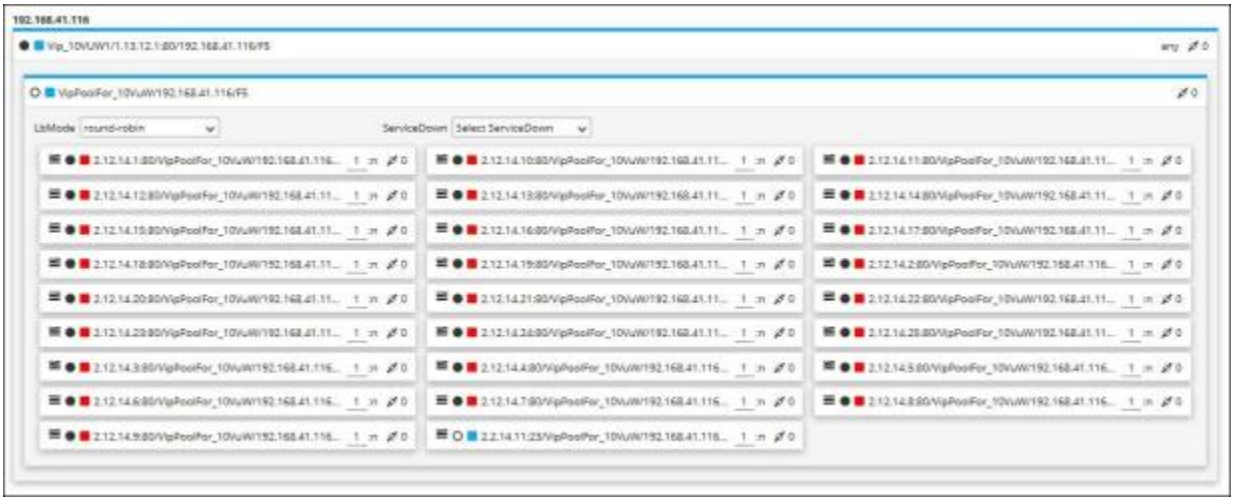
There are two ways to view additional details about search results and the method varies depending on the type of object you are viewing:

- ADC, Certificate, and SSH primary object search results are clickable and take you to topological screens that provide much more information about the corresponding object than is displayed on the search results screen.
- ADC primary and secondary object search results can be right-clicked to view the list of actions available for them.
- Firewall, WAF, and Proxy search results are not clickable and include only the information contained on the search results screen.

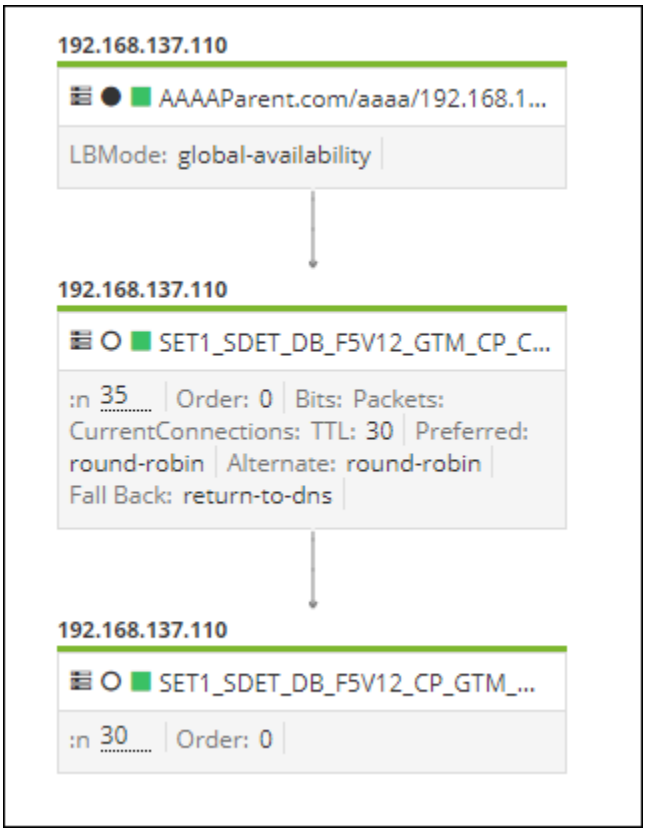
### ADC Primary Object Topological Views

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 module.

### Virtual Server (VIP) Topology

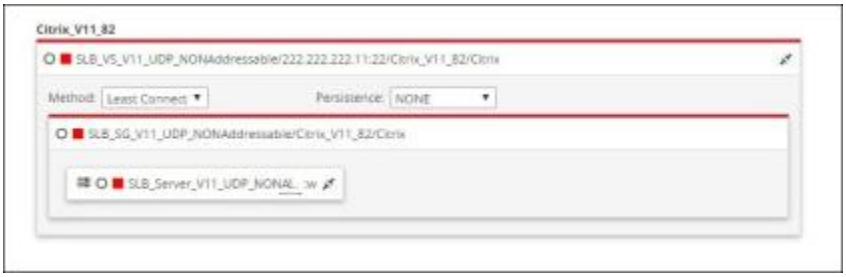


### Wide IP Topology

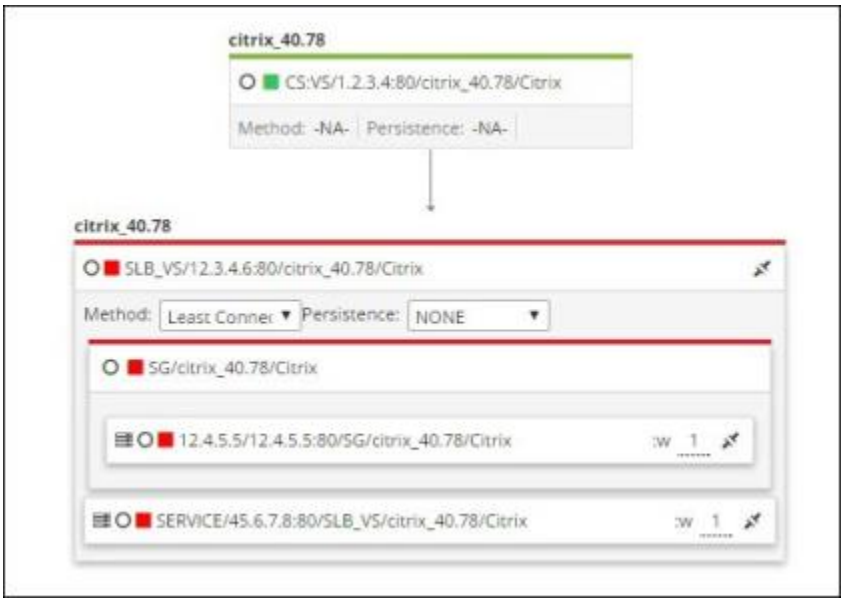



**Global Server Load Balancing (GSLB) Virtual Server Topology**

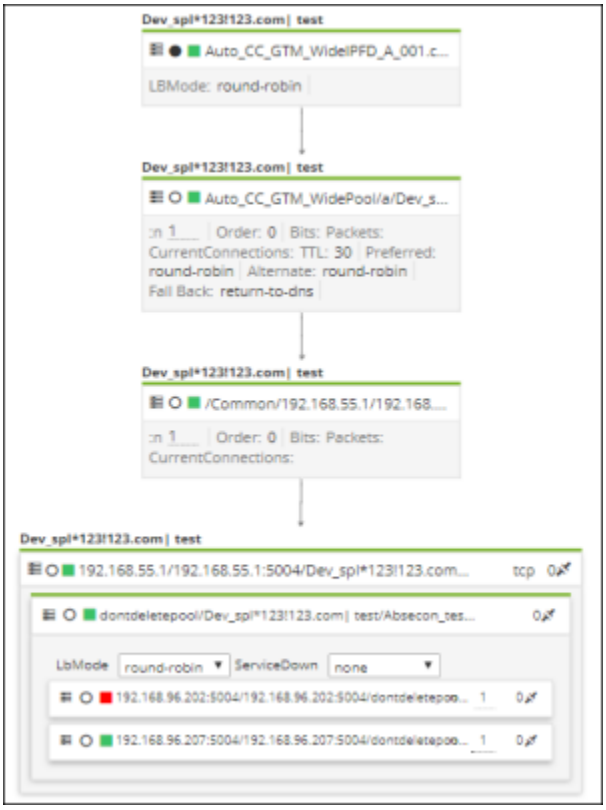

**Server Load Balancing (SLB) Virtual Server Topology**



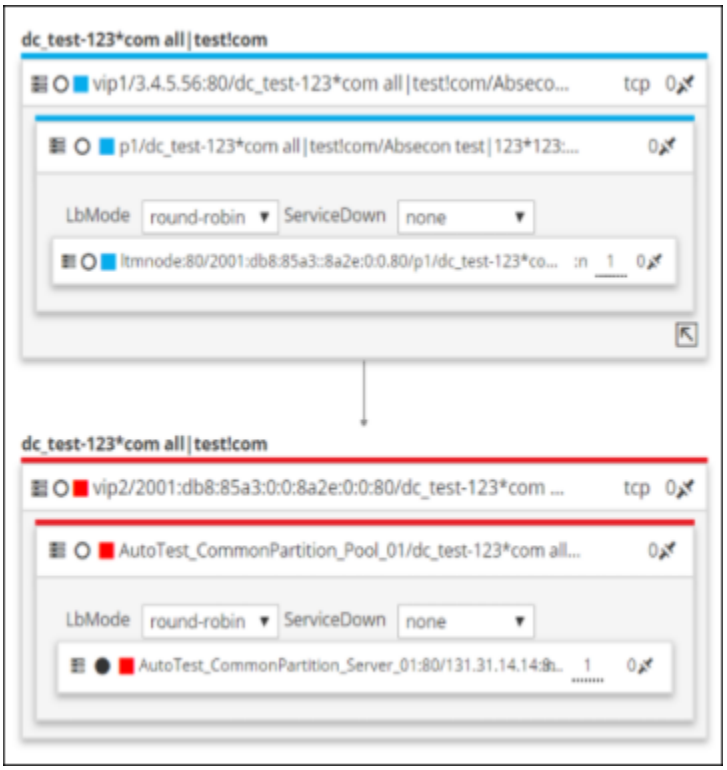

**CS Virtual Server Topology**




**Virtual Server (VIP) under Wide IP Topology**




**Virtual Server IP (VIP) under VIP topology**



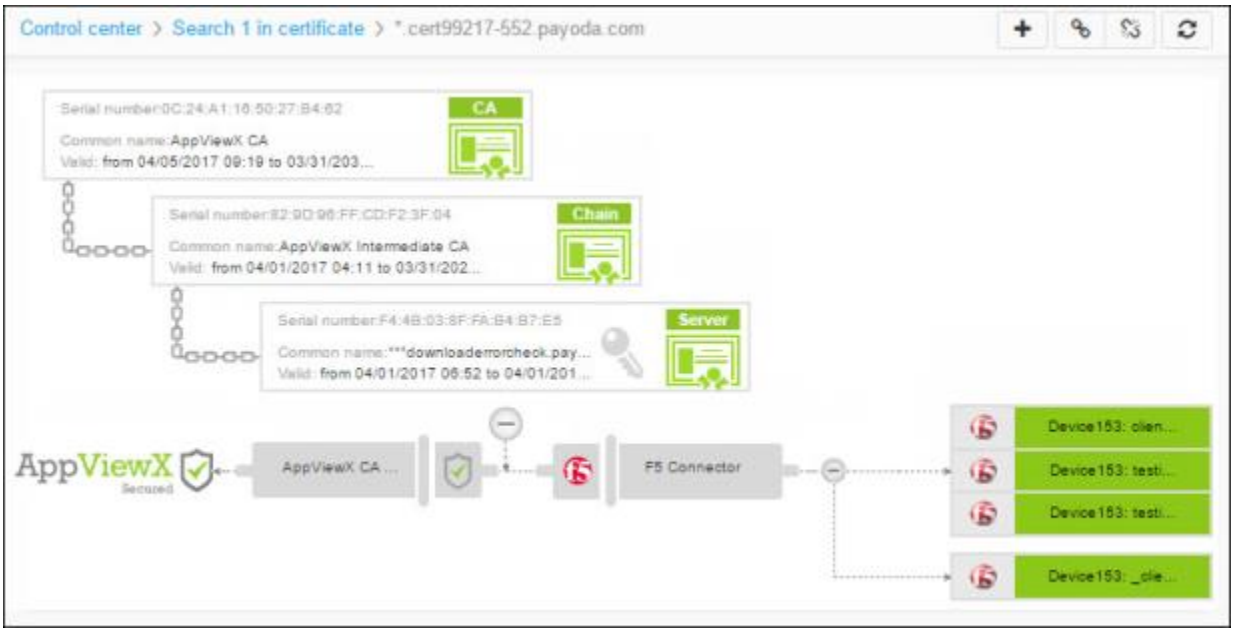

**ADC Primary and Secondary Objects Additional Details**

When you run a search for an ADC secondary object-such as an iRule, a policy, or a class- you can perform various actions on the search results.

For a detailed description of the features and functionalities available within the ADC search result screen, refer to the ADC Topology Actions section of this guide.

**Certificate Topological Views**

When you click the **Server certificate**, **Client certificate**, or **Code signing** certificate tab to view the search results corresponding to your search query, a topology view opens, providing a detailed map showing the trust chain that extends from the root certificate to intermediate certificates to the end certificate itself. This view also shows the relationship between all of the other components related to the certificate, including connectors and devices.



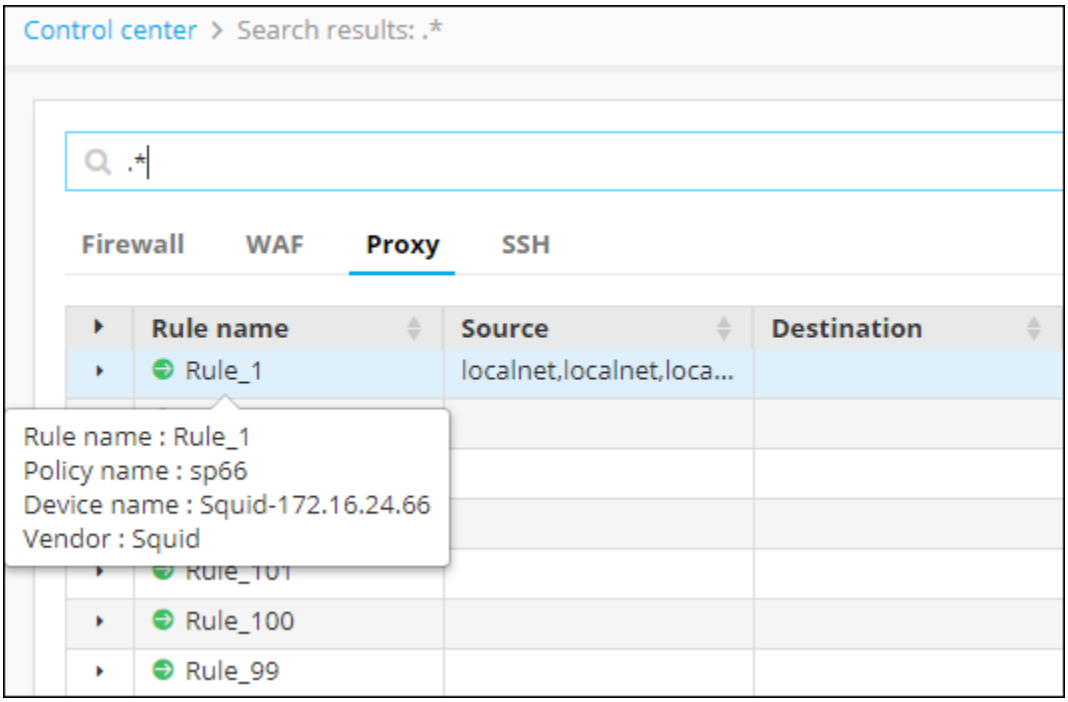

### Firewall and WAF Additional Details

Most of the details of Firewall and WAF objects are visible directly on the search results screen. However, some columns within the search results contain icon that open popup screens that provide Read-Only access to the specific settings for the corresponding object parameter. For more details, refer to the View the Settings for WAF Threat Protection and View the Nested Groups for a Firewall Rule section of this guide.

### Proxy Additional Details

The details of Proxy objects do not appear on separate screens or popup screens as they do for other objects. Instead, all of the additional information is made available without leaving the search results screen. Not all of the information is immediately visible, however, depending on the rule type listed in the search results, you might be able to view additional information by doing the following:

- Hovering your cursor over a rule name. Note that this functionality is available for all object types, not just Proxy ones.



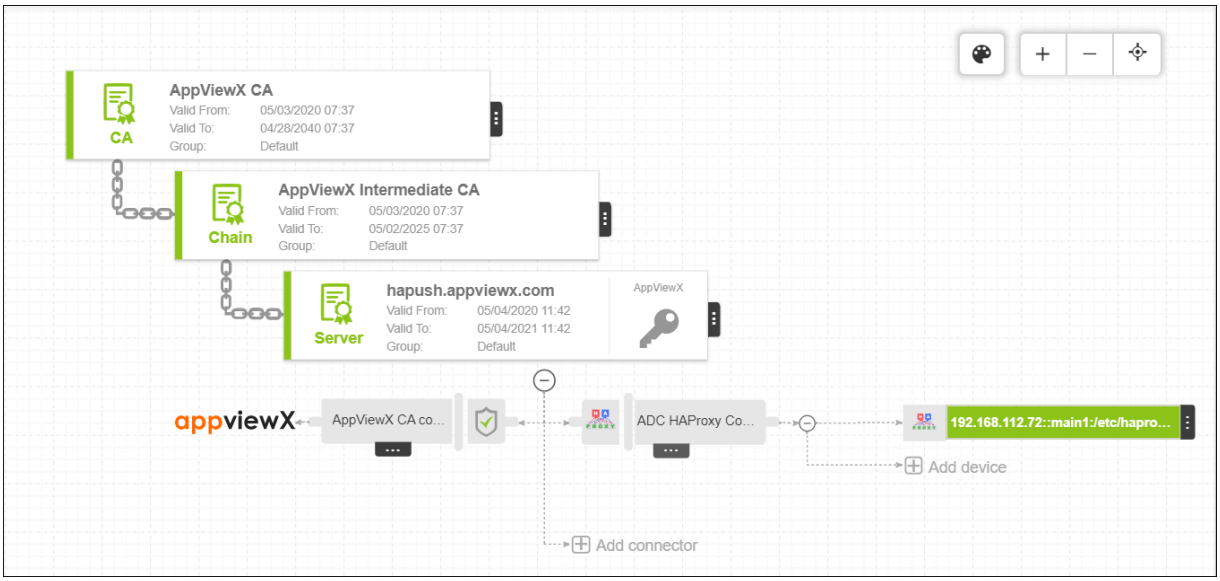

- Clicking ▸ that appears in the first search results column. Note that this functionality is available for all object types, not just Proxy ones. In addition, although each row contains an Expand icon, if all of the details fit within the standard height of a results row, the row will not get any taller when you click the icon.

## View the Certificate Search Results

To view the certificate search results within the Control Center:

1. Run a search.
2. Click the **Server Certificate**, **Client Certificate**, or **Code Signing Certificate** tab to view the search results corresponding to your search query.
   When you click a search result from any of the tabs, a topology view opens, providing a detailed map showing the trust chain that extends from the root certificate to intermediate certificates to the end

certificate itself. This view also shows the relationship between all of the other components related to the certificate, including connectors and devices.




## 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 button.


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.

   The screen then refreshes and filters the results on both the Application view and Infrastructure view based on the filter you selected.

# Export the ADC and SSH Search Results

This feature is available only for the ADC objects and SSH keys.

To export all **ADC** search results within the Control Center:

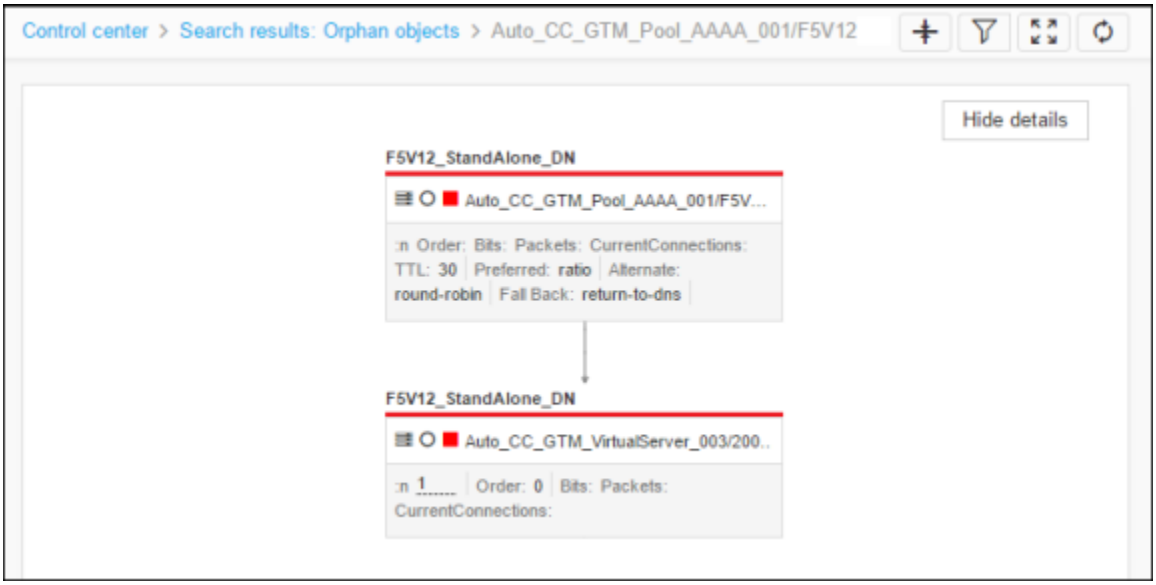
1. Run a search.
2. By default, the search results are displayed in the Application view.
3. Click  beside the object name to select the object details that you want to export from the grid or select all of the ADC objects by clicking  in the Command bar.
4. All of the search results on the screen display with a blue background to indicate that they have been selected.
5. Click  in the Command bar.
6. The **.csv** file is downloaded to your computer.
7. Go to the location where you want to file to go, then click Save.
8. The ADC Parent, Child 1, and Child 2 object details, as well as the state and status of all of the objects, are then exported to your computer.
9. If you want to export the search results displayed on the infrastructure view, click  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  in the Command bar.
   - On the **Export** screen that pops up, select either the **All columns** or **Displayed columns** radio button based on what you want to export from the grid.
   - The **.csv** file is downloaded to your computer.
   - Navigate to the location where you want to file to go, then click Save.
10. To export all the **SSH** search results within the Control Center, run a search.
    By default, the search results are displayed on the Application view page.
11. Click the **SSH** tab.
12. In the list of key names, click the checkbox beside the key name you want to export.
13. Click  in the Command bar.
14. On the pop-up screen that opens, choose whether you want to export all columns of data or just the columns that are currently visible on the SSH tab.
15. Choose whether to save the exported certificate as a **CSV** or an **XLS** file.
16. Click **Export**.
17. Select the location where you want to export the file, then click **Save** to complete the export.

# View Orphan Objects

This feature is available only for ADC device objects.

To view orphan objects through the Control center module, complete the following steps:

1. Click and select Control Center.
2. Run a search.
3. On the search results screen that opens, click or on which you want to view the orphan objects.
4. Click n in the Command bar at the top of the screen.
   The Orphan objects screen opens, displaying all orphan objects grouped by device type.
5. Click the tab that corresponds to the type of orphan object you want to view.
6. Hover your cursor over any of the child objects to view its details.
7. Click any of the child objects to view the topology the object belongs to.




# 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 .

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.


   The topology updates and no longer displays the information you filtered out.
4. To turn off filters, repeat the steps above, but select, rather than deselect, the type of information you want to view.

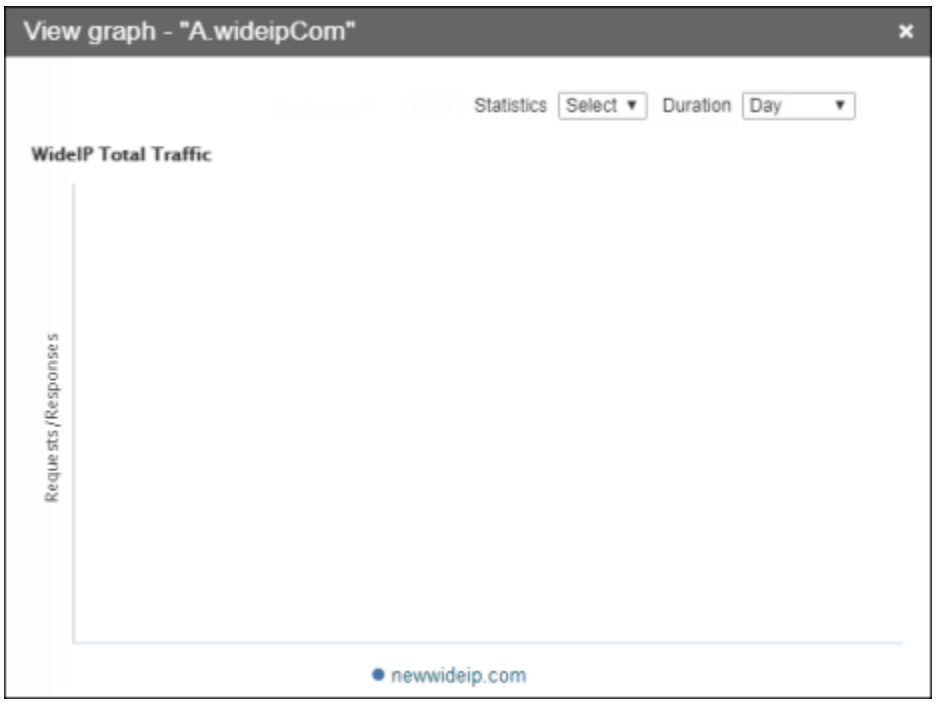
## View Timeline Statistics for an Object

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

1. Click and select Control Center
2. Run a search.
3. By default, the search results are displayed in the **Application view** page.
4. Right-click the device name and select **View** > **View graph** from the dropdown list that appears.
5. If you want to view the statistics for the search results displayed on the infrastructure view, click to switch from the Application view search result page.
6. 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 Configuration Details

**Note:** This feature is available only for the ADC device objects, Firewall rules, and WAF devices.

- View Configuration Details of ADC Device Objects
- View Configuration Details of Firewall Rules
- View Configuration Details of WAF Devices

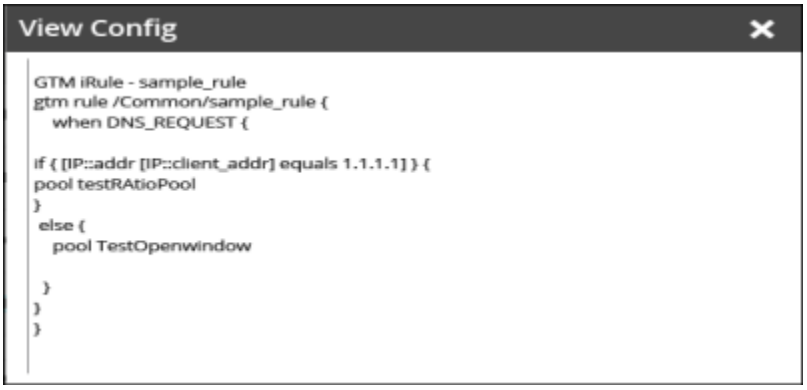
## View Configuration Details of ADC Device Objects

1. Click and select **Control Center**.
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  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 Configuration Details of Firewall Rules

1. Click  and select **Control Center**.
2. Run a search.
3. By default, the search results are displayed in the **ADC Application view** page.
4. Click the **Firewall** tab.
5. On the search results screen, right-click the device name and select View config from the dropdown list that appears.

A popup screen appears, displaying the configuration details as shown in the image below:


## View Configuration Details of WAF Devices

1. Click ☰ and select **Control Center**.
2. Run a search.

   By default, the search results are displayed in the **Application view** page.
3. Click the **WAF** tab.
4. On the search results screen, right-click the device name and select View config from the dropdown list that appears.

A popup screen appears, displaying the object's configuration as shown in the image below:

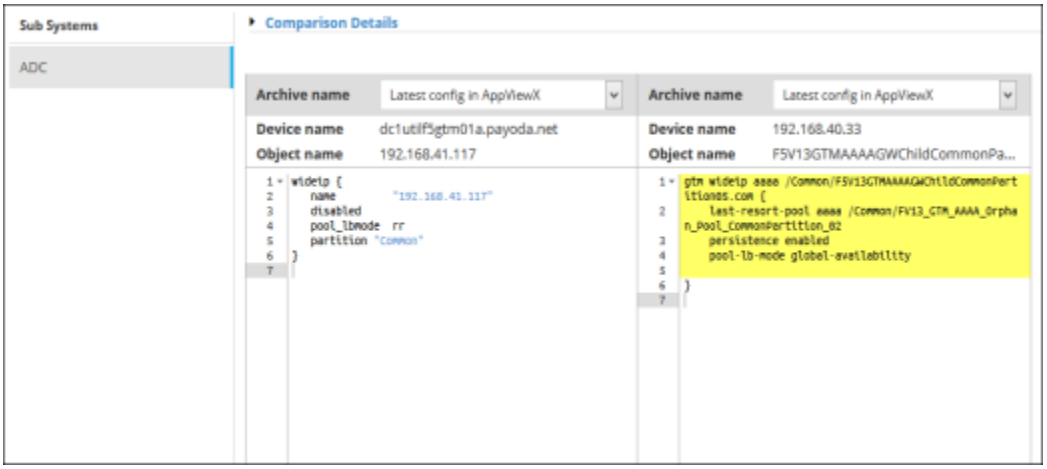

## Compare ADC Objects

- 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 Control Center:

1. Click and select Control Center.
2. Run a search.
   By default, the search results are displayed in the Application view page.
3. Click 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 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**.

The screen refreshes and displays the archived configurations side-by-side.




## Filter Firewall Search Results

To filter Firewall search results within the Control Center:

1. Run a search.
2. On the search results screen, click the **Firewall** tab
3. Click the dropdown menu that appears beside the search bar.
4. Select one of the three filter options in the dropdown list that appears:
   - Security - The search results will display only the Security rules.
   - NAT - The search results will display only the NAT rules.
   - Route - The search results will display only the Static routes.

## Create a Rule or Route

To create a Security Rule, NAT Rule, or Static Route Rule:

1. Click ☰ and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. Select one of the following three filter options from the dropdown list depending on what you want to create:
   - **Security**
   - **NAT**
   - **Route**

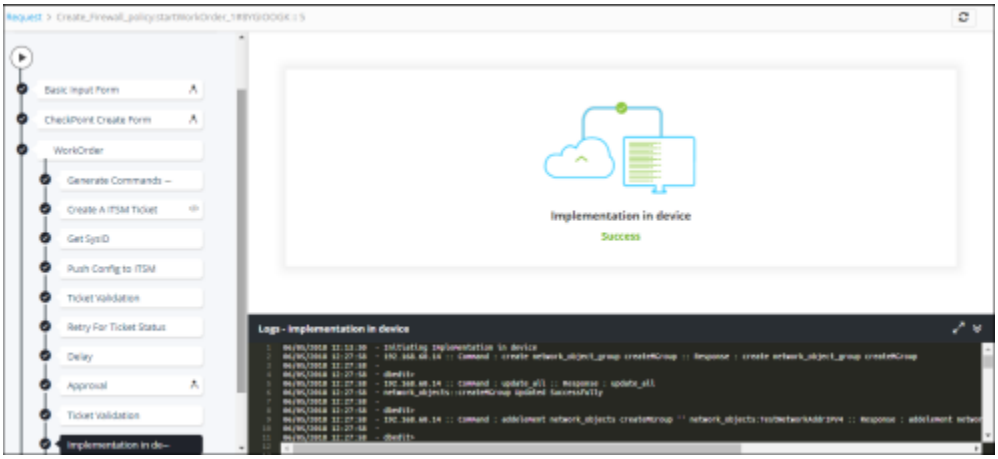
5. Click  in the Command bar.

   The **Basic Input Form** opens with the **Request View** tab selected by default.
6. Fill in all the form fields designated with a * beside their names.
7. Click **Submit** to trigger the workflow.

   A new **Request ID** is created. To view the request details, refer to the Request Tasks section of this guide. The create form corresponding to the **Vendor** you selected in *Basic Input Form* and the filter option selected in step 5. will be displayed.
8. At a minimum, fill in all the form fields designated with a * beside their names.
9. Click **Submit**.

   The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the Logs pane at the bottom of the screen. After you submit the request form, the configuration changes are reviewed and approved at AppViewX.
10. Enter any comments you have related to the implementation and then, click **Implement**.

    The configuration commands are implemented, resulting in the creation of a rule or route in the device.




## Modify a Rule or Route

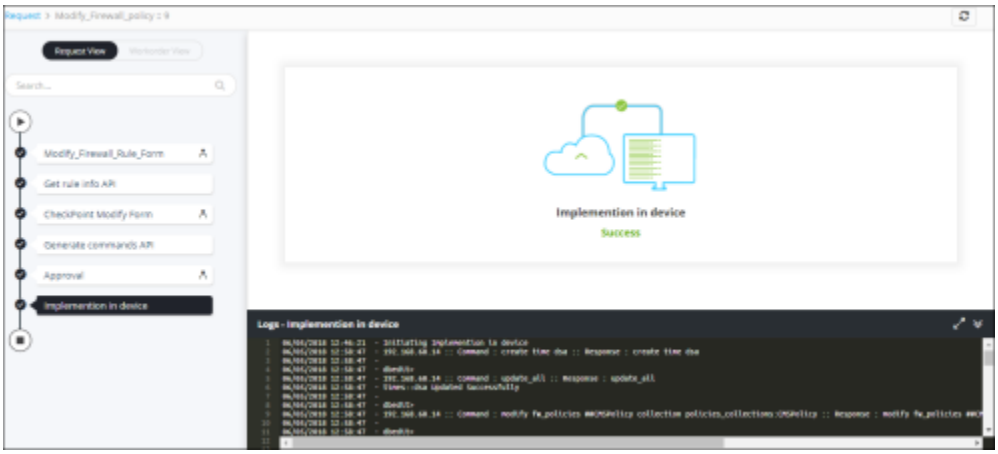
To modify a Security Rule, NAT Rule, or Static Route Rule:

1. Click  and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. Select one of the following three filter options from the dropdown list depending on what you want to modify:

- **Security**
- **NAT**
- **Route**

The screen then refreshes and displays the results based on the filter you selected.

5. Right-click the rule name and select **Modify** from the dropdown list that appears.
6. Enter a search key for the rule you want to modify and then, click **Submit**.
   This will trigger the workflow and a new **Request ID** is created. To view the request details, refer to the Request Taskssection of this guide. The information regarding the rule you trying to modify is fetched using API and the **modify** form for the corresponding rule will be displayed.
7. Make whatever changes you want to the rule by filling in the form fields designated with * beside their names.
8. Click **Submit**.
   The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen. After you submit the request form, the configuration changes are reviewed and approved at AppViewX.
9. Enter any comments you have related to the implementation and then, click **Implement**.
   The configuration commands are implemented, resulting in modifying the rule or route in the device.




## Delete a Rule or Route

To delete a Security Rule, NAT Rule, or Static Route Rule:

1. Click and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.

4. Select one of the following three filter options from the dropdown list depending on what you want to delete:
   - **Security**
   - **NAT**
   - **Route**

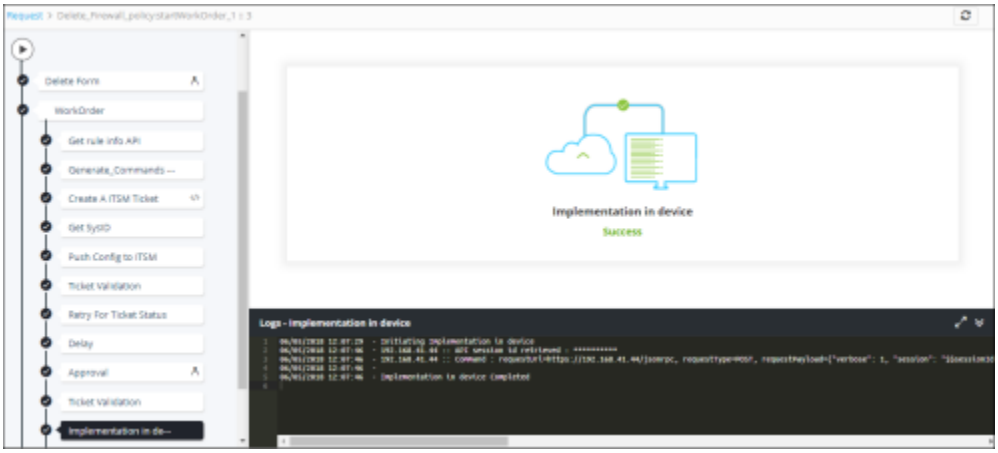
   The screen then refreshes and displays the results based on the filter you selected. Right-click the rule name and select **Delete** from the dropdown list that appears.

> **Note:** Ensure that the ITSM device (Service Now) is registered in AppViewX. For more details, refer to the Change Managementsection of this guide.

5. On the **Delete Rule** screen that pops up select one of the following actions based on how you want to trigger the workflow:
   - **Confirm with CR ticket** - Creates an ITSM ticket using Service Now for tracking and approval purpose.
   - **Confirm without CR ticket** - Deletes a rule without creating an ITSM ticket using Service Now for tracking and approval purpose.
   - **Discard request** - Exits the Delete Rule screen.
6. Click **Ok** to trigger a workflow.

   A new **Request ID** is created. To view the request details, refer to the Request Taskssection of this guide. The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the Logs pane at the bottom of the screen. The information regarding the rule you trying to delete is fetched using API and the configuration changes are reviewed and approved at AppViewX.
7. Enter any comments you have related to the implementation and then, click **Implement**.

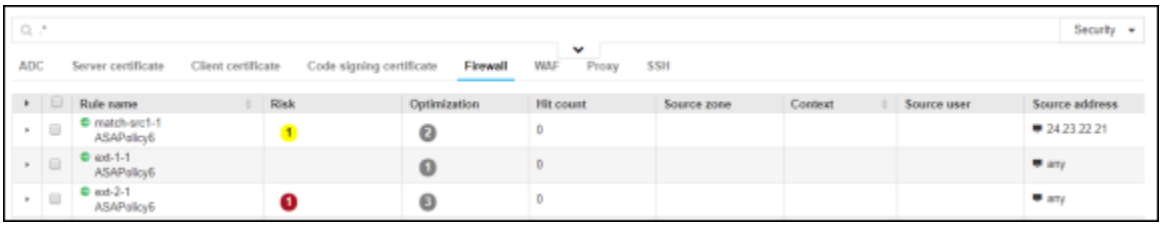
   The configuration commands are implemented, resulting in deleting the rule or route from the device.



# Compare Firewall Rules

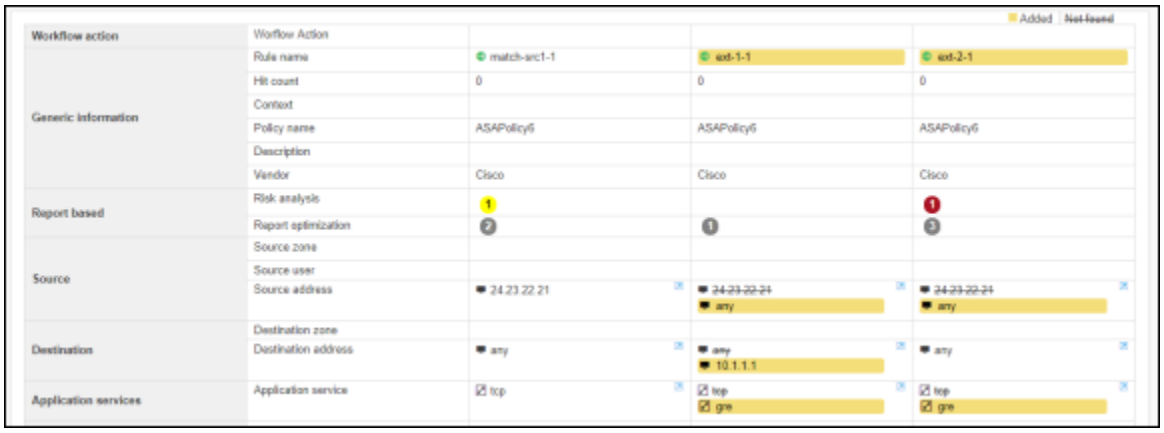
To compare firewall rules within the Control Center:

1. Click ☰ and select **Control Center**.
2. Run a search for the Firewall rules (either Security Rules, NAT rules, or Route Rules) you want to compare.
3. On the search results screen, click the Firewall tab.
4. In the search results field, select up to three Firewall rules that you want to use in the comparison.




5. Click ⇄ in the Command bar.
6. On the Select primary policy popup screen that appears, select the radio button beside the Firewall rule that you want to use as the basis of the comparison, then click **Compare**.
   The Firewall rule details then appear side-by-side on the Compare policies screen with the following markups:
   - Yellow highlights are used to indicate different content between the two rules. In the image below, the name of the secondary rule differs from the first, so it is highlighted. Highlighting is also used to indicate content that appears only in the secondary or tertiary rule.
   - Strike-through text is used to indicate rule components that appear in the primary rule but are absent in the second and/or third rule. In the image below, the primary rule lists **HTTPS** and **TCP** as the

Firewall protocols, but the secondary policy does not contain any protocols so those values are struck out.

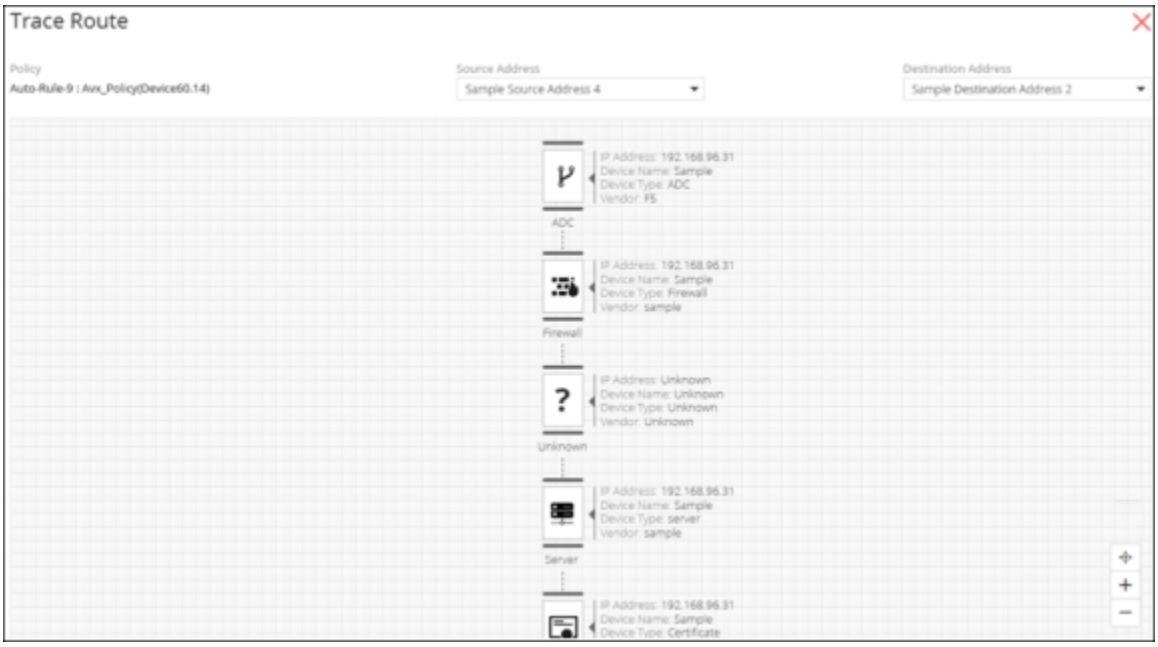



**Note:** If the **HTTPS** and **TCP** protocols had appeared only in the secondary policy, they would have appeared as highlighted text rather than strike-through text.

## View the Trace Route Details

To view the traceroute details between the source and destination address of a rule:

1. Click ☰ and select Control Center
   The Control center screen opens.
2. Run a search.
3. On the Search results screen that opens, click the **Firewall** tab.
4. Right-click the rule name and select **Traceroute** from the dropdown list. The **Traceroute** screen for the respective rule opens.
5. Select the **Source Address** and the **Destination Address** from the respective dropdown fields and then, click **Go**.
   The Traceroute is executed and the hops between the source and destination address will be plotted in the grid space.

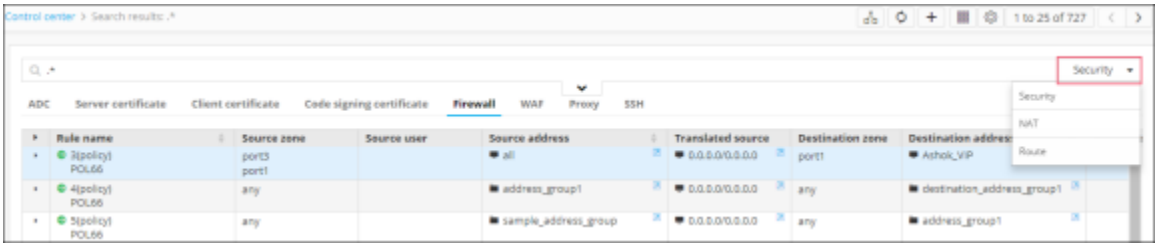



6. Click  in the command bar if you want to configure the number of ping responses and hidden hops you want to be displayed in the grid space.

## View the Route Details

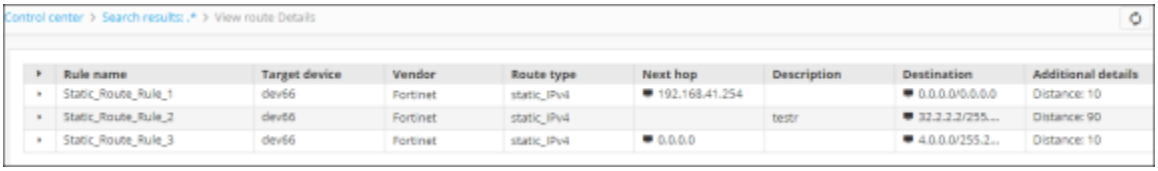
To view the static route details for a security rule:

1. Click  and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. Select **Security** from the dropdown list, if it is not already selected.
   The list of all the available security rules is displayed.




5. Right-click the rule name and select **View Route details** from the dropdown list that appears.

**Static Routes** that are created for the security rule will be displayed.

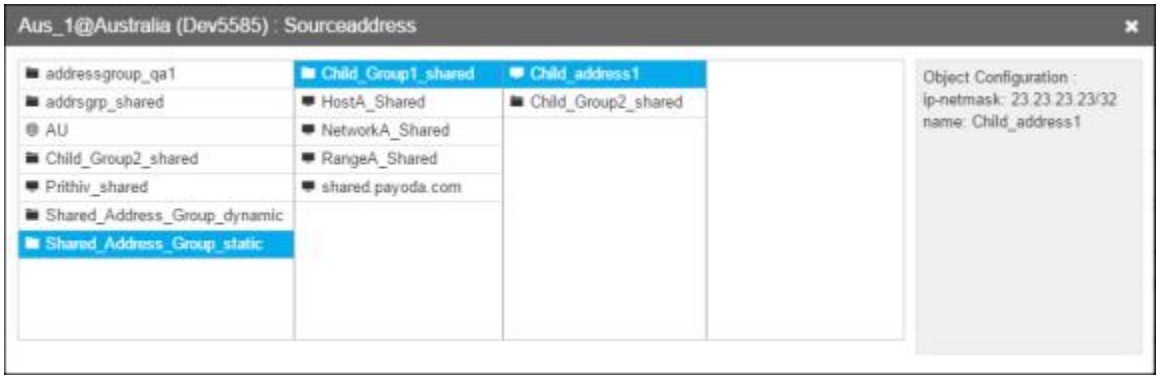



## View the Nested Groups for a Firewall Rule

To view the nested groups corresponding to a firewall rule:

1. In the Control center module, run a search for the firewall whose rule details you want to view.
2. In the search results field, locate the rule.
3. Click in the source address, a destination address, translated destination, application/services, translated service, or schedule column, depending on which rule parameter you want to view.
   On the popup screen that appears, the top-level groups appear in the left column.

   - If a group has no nested groups, its details appear in the far-right column.
   - If a group has nested groups, the nested groups appear in a new column that appears to the right. If the nested groups also have nested groups, those will appear in another new column, which appears to the right of the original nested groups' column.



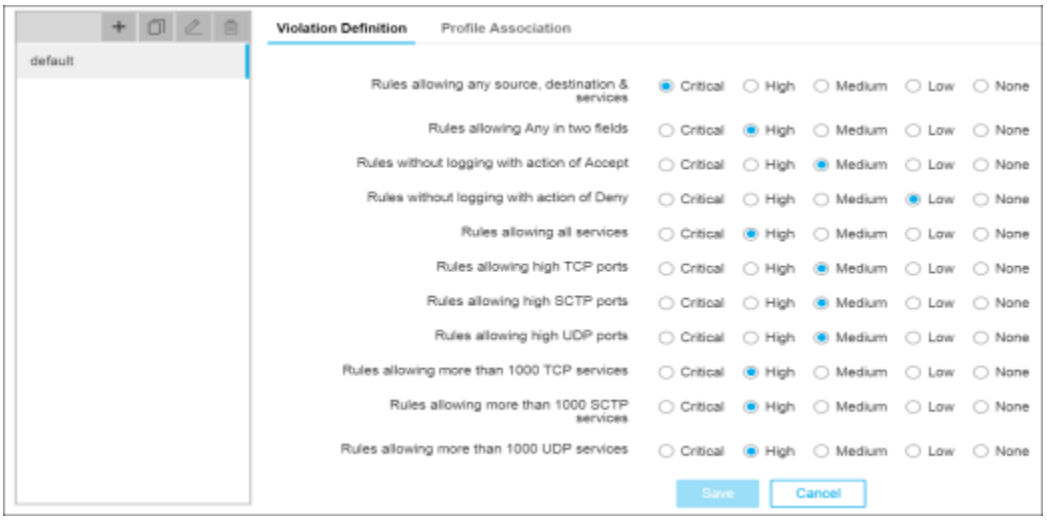

## Configure Firewall Risk Settings

Configuring the risk settings enables the user to define a set of violations and associate it with the profiles, based on which the risk reports will be generated. These reports can be used to mitigate the risks at an infrastructure or application level.

**Note:** Click  and configure the level (based on which the risk reports are generated in the Control Center module) you want to use for profile association.

To configure the firewall risk settings:

1. Click and select **Control Center**.
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. Click  in the Command bar.
5. On the **Risk Report Settings** screen that opens, click the **Violation Definition** tab if it not displayed by default.
   The predefined set of violations under the **default** category is displayed.




6. Modify the severity of the existing violations by clicking the corresponding radio buttons as required.
7. (Optional) If you want to add a new violation:
   a. In the **Custom Violations** section, enter a name for the violation to help the users identify it.
   b. From the **Parameters** dropdown list, select the parameter based on which you want the risk report to be generated.
   c. In the **Operators** dropdown list, select either **equal to** or **not equal to** option depending on whether you want the parameters and the values provided to be an exact match.
   d. Enter a value for the parameter you selected in Step 7. b.
   e. In the **Operators** dropdown list, select the **AND** or **OR** option depending on whether you want to use a boolean operator between the parameters you set for the violation.
   f. From the **Risk** dropdown, select the severity that must be associated with the parameter.

g. Click the **Add** button to create a new violation.

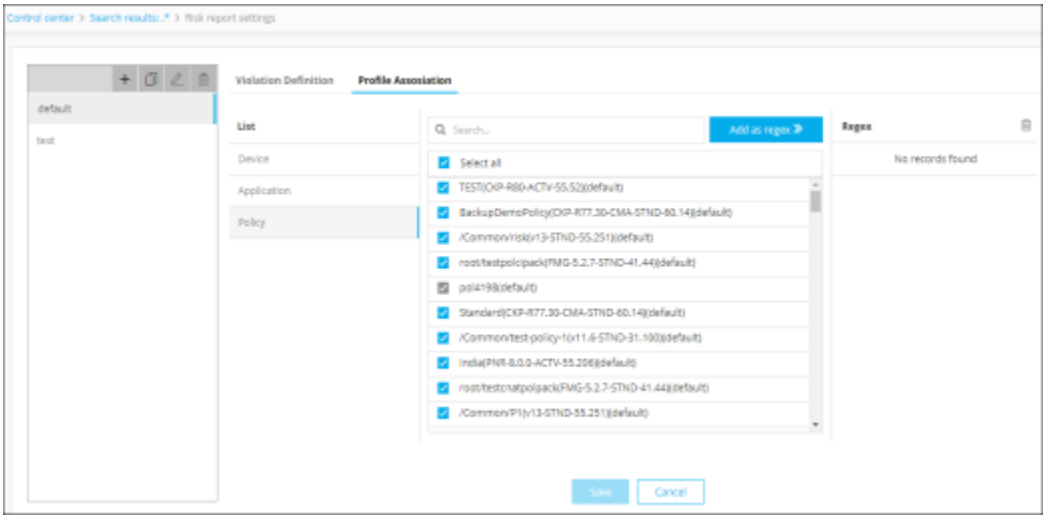
h. You can delete or modify the custom violation details by clicking either  or  .

i. Click **Add** and repeat Step 7.a. through 7.f. to add more violations to the corresponding category.

8. Click **Save**.

   A new category is created which displays all the configured violations and its severity.

9. Click the **Profile Association** tab.




10. Select any one of the following levels under the **List** section, to associate their profiles with the category.
    - **Device**
    - **Application**
    - **Policy**
11. Select the checkbox beside the profiles and then, click **Save**.
12. If you want to use a **regular expression** (**regex**) to identify the profiles you want to associate with the category, enter the regex in the **Search** field, then click the **Add as regex** button. The list updates and shows checkmarks beside all profiles that match the regex to indicate that they have been selected. The **Regex** column also displays the total number of profiles that match each of the regex search criteria you have created.

    The risk reports are generated based on the set of violations and its associated profiles you configured. The **Risk** column in the search results screen will display the risk reports for each rule.
13. (Optional)To create more category of violations, follow these steps:

    a. Click  on the left-hand side of the screen.

    b. Click  . All the predefined violations available under the default category is displayed.

    c. Enter a name for the category to help the users identify it.

    d. Repeat Step 8. through 13.

14. (Optional) To create an exact copy of the existing category, follow these steps:

    a. Select the category on the left-hand side of the screen.

    b. Click  .

    The cloned category is created with all the violations and its associated profiles the same as the category you selected in Step 15.a.

15. (Optional) To rename a category, follow these steps:
    a. Select the category on the left-hand side of the screen.
    b. Click  .
    c. Modify the name of the selected category and then, click  .
16. (Optional) To delete the category, follow these steps:

    a. Select the category on the left-hand side of the screen.

    b. Click  .

    c. In the **Confirmation** dialog box, click **Delete**.

    All the corresponding violations and their associated profiles will be deleted.

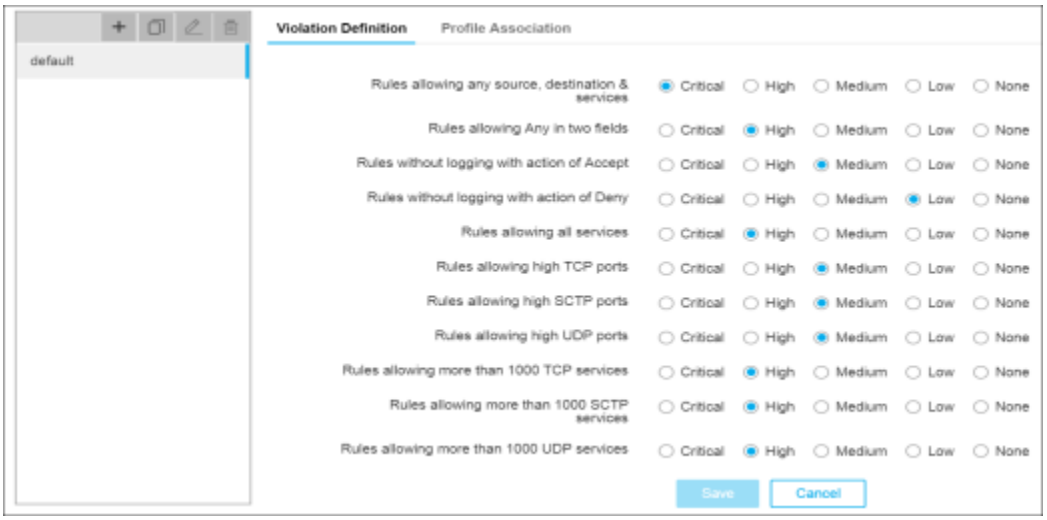
## Configure WAF Risk Settings

Configuring the risk settings enables the user to define a set of violations and associate it with the profiles, based on which the risk reports will be generated. These reports can be used to mitigate the risks at an infrastructure or application level.

To configure the WAF risk settings:

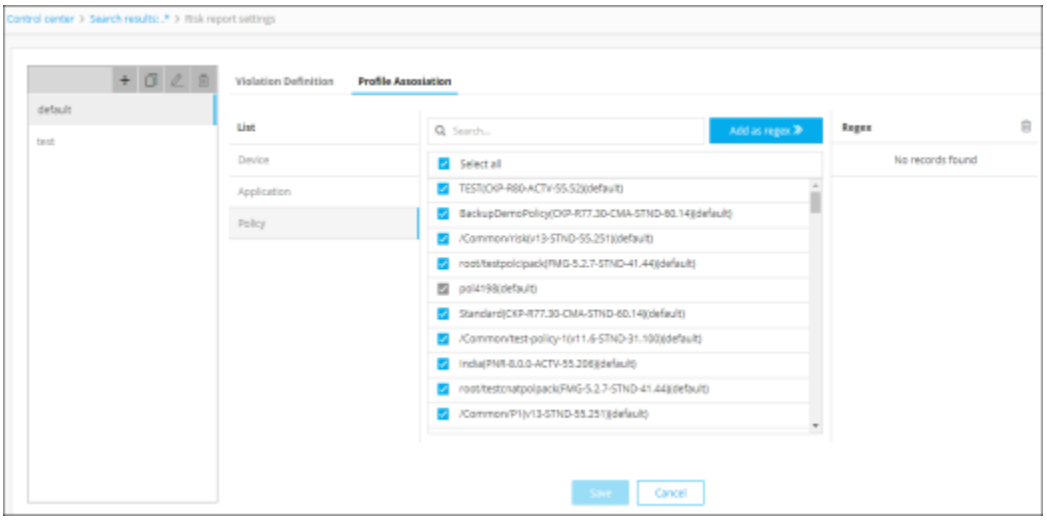
1. Click  and select **Control Center**.
2. Run a search.
3. On the search results screen that opens, click the **WAF** tab.
4. Click  in the Command bar.
5. On the **Risk Report Settings** screen that opens, click the **Violation Definition** tab if it not displayed by default.

   The predefined set of violations under the **default** category is displayed.




6. Modify the severity of the existing violations by clicking the corresponding radio buttons as required.
7. (Optional) If you want to add a new violation, do the following:
   a. In the **Custom Violations** section, enter a name for the violation to help the users identify it.
   b. From the **Parameters** dropdown list, select the parameter based on which you want the risk report to be generated.
   c. In the **Operators** dropdown list, select either **equal to** or **not equal to** option depending on whether you want the parameters and the values provided to be an exact match.
   d. Enter a value for the parameter you selected in Step 7. b.
   e. In the **Operators** dropdown list, select the **AND** or **OR** option depending on whether you want to use a boolean operator between the parameters you set for the violation.
   f. From the **Risk** dropdown, select the severity that must be associated with the parameter.
   g. Click the **Add** button to create a new violation.
   h. You can delete or modify the custom violation details by clicking either  or  .
   i. Click **Add** and repeat Step 7.a. through 7.f. to add more violations to the corresponding category.
8. Click **Save**.

   A new category is created which displays all the configured violations and its severity.
9. Click the **Profile Association** tab.




10. Select any one of the following levels under the **List** section, to associate their profiles with the category.
    - **Device**
    - **Application**
11. Select the checkbox beside the profiles and then, click **Save**.
12. If you want to use a **regular expression** (**regex**) to identify the profiles you want to associate with the category, enter the regex in the **Search** field, then click the **Add as regex** button. The list updates and shows checkmarks beside all profiles that match the regex to indicate that they have been selected. The **Regex** column also displays the total number of profiles that match each of the regex search criteria you have created.
    The risk reports are generated based on the set of violations and its associated profiles you configured. The **Risk** column in the search results screen will display the risk reports for each rule.
13. (Optional)To create more category of violations, follow these steps:
    a. Click  on the left-hand side of the screen.
    b. Click  . All the predefined violations available under the default category is displayed.
    c. Enter a name for the category to help the users identify it.
    d. Repeat Step 8. through 13.
14. (Optional) To create an exact copy of the existing category, follow these steps:
    a. Select the category on the left-hand side of the screen.
    b. Click  .
    The cloned category is created with all the violations and its associated profiles the same as the category you selected in Step 15.a.

15. (Optional) To rename a category, follow these steps:
    a. Select the category on the left-hand side of the screen.
    b. Click  .
    c. Modify the name of the selected category and then, click  .
16. (Optional) To delete the category, follow these steps:
    a. Select the category on the left-hand side of the screen.
    b. Click  .
    c. In the **Confirmation** dialog box, click **Delete**.
    All the corresponding violations and their associated profiles will be deleted.

## View the Hit Count for a Firewall Device

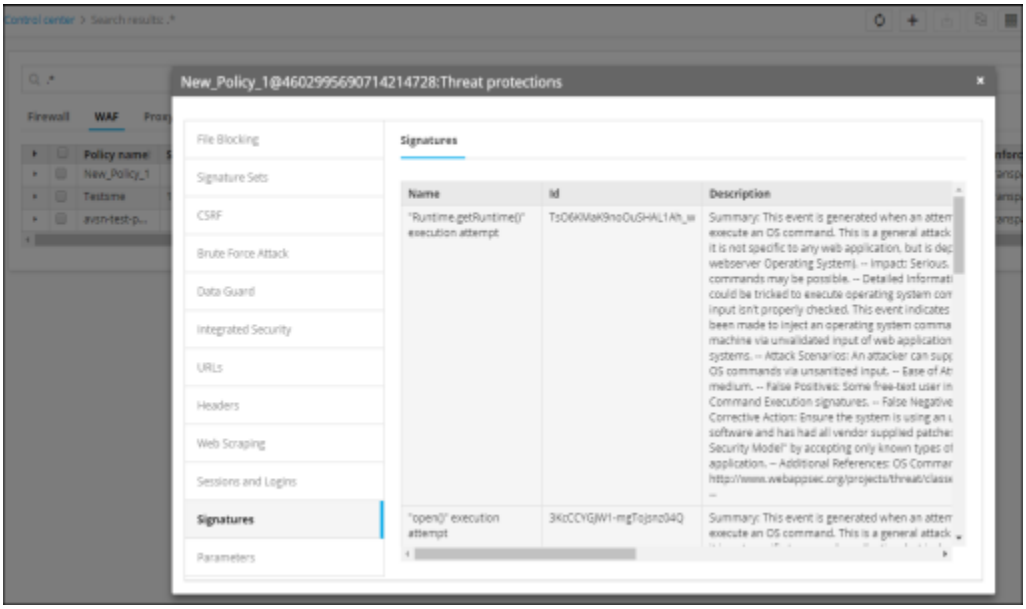
To view the hit counts for F5, Cisco, Juniper, and some CheckPoint firewall devices in the AppViewX system, complete the following steps:

1. Click  and select **Control Center**.
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. If the device whose hit count you want to view is not visible on the screen, run a search to locate it.
5. In the search results field, the Hit count column displays the number of hits the corresponding firewall has received.
6. If the column is not visible even after you scroll to the right, complete the following sub-steps to display it:
    a. In the Command bar, click  .
    b. On the Columns screen that pops up, locate Hit Count in the Available column and click » beside it to move it to the Assigned column.
    c. Click **Save**.
    The results field then refreshes and displays the column. Note again that you might have to scroll right to see the column.

# View the WAF Threat Protection Settings

To view the threat protections settings for a WAF:

1. In the Control center module, run a search for the WAF whose details you want to view.
2. In the search results field, locate the rule.
3. Click in the **Threat Protection** column.
4. On the popup screen that appears, various settings of the Threat Protections parameter are displayed in the left column.
   Clicking any of the tabs on the left side of the popup screen, such as File Blocking, Signature Sets, CSRF, Brute Force Attack, Data Guard, Integrated Security, URLs, Headers, Web Scraping, Sessions and Logins, Signatures, or Parameters, causes the corresponding settings to appear on the right side of the screen.




# Create a WAF Policy

To create a WAF policy:

1. Click and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **WAF** tab.
4. Click in the Command bar.
   The **ASM Policy Creation Form** opens with the **Request View** tab selected by default.
5. Fill in all the form fields designated with a * beside their names.

6. Click **Submit** to trigger the workflow.
   A new **Request ID** is created. To view the request details, refer to the Request Tasks section of this guide. The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.
7. After you submit the request form, the configuration changes are reviewed and approved at AppViewX.
8. Enter any comments you have related to the implementation and then, click **Implement**.
   The configuration commands are implemented, resulting in the creation of a rule or route in the device.

## Download a WAF Policy

To download the WAF policies:

1. Click and select Control Center
2. Run a search.
3. On the search results screen, click the WAF tab.
4. Select the checkbox beside the policy name you want to download.

> **Note:** You can select all of the policies by clicking the first checkbox in the grid.

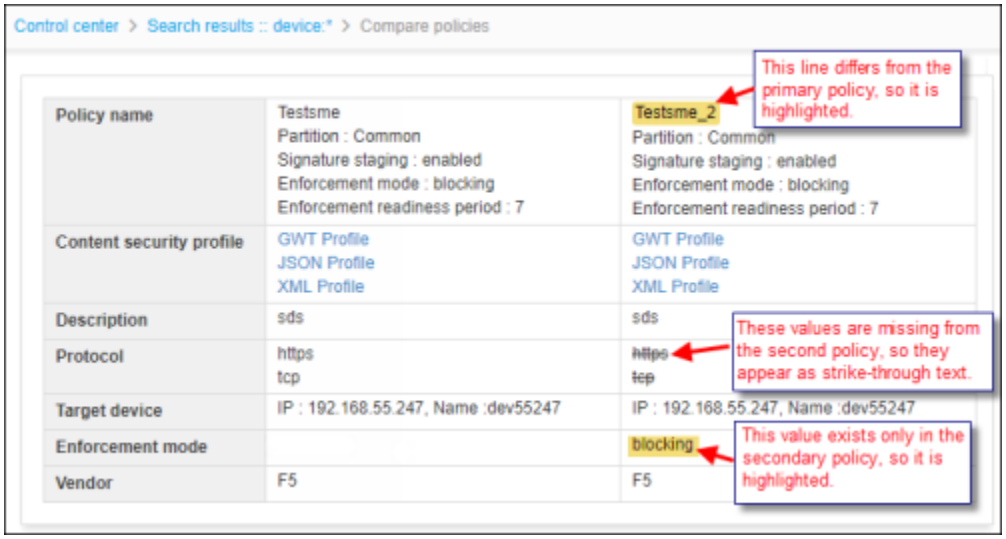
5. Click in the Command bar.
   The selected policy will download to your computer.
6. Select the file and navigate to the location where you want the file to go, then click **Save**.

## Compare WAF Policies

To compare WAF policies within the Control Center,

1. Click and select Control Center
2. Run a search for the WAF policies you want to compare.
3. On the search results screen, click the WAF tab.
4. In the search results field, select up to three WAF policies that you want to use in the comparison.

5. Click in the Command bar.
6. On the Select primary policy popup screen that appears, select the radio button beside the WAF policy that you want to use as the basis of the comparison, then click Compare.
   The WAF policy details then appear side-by-side on the Compare policies screen with the following markups:
   - Yellow highlights are used to indicate different content between the two policies. In the image below, the name of the secondary policy differs from the first, so it is highlighted. Highlighting is also used to indicate content that appears only in the secondary or tertiary policy.
   - Strike-through text is used to indicate policy components that appear in the primary policy but are absent in the second and/or third policy. In the image below, the primary policy lists **HTTPS** and **TCP** as the WAF protocols, but the secondary policy does not contain any protocols so those values are struck out.



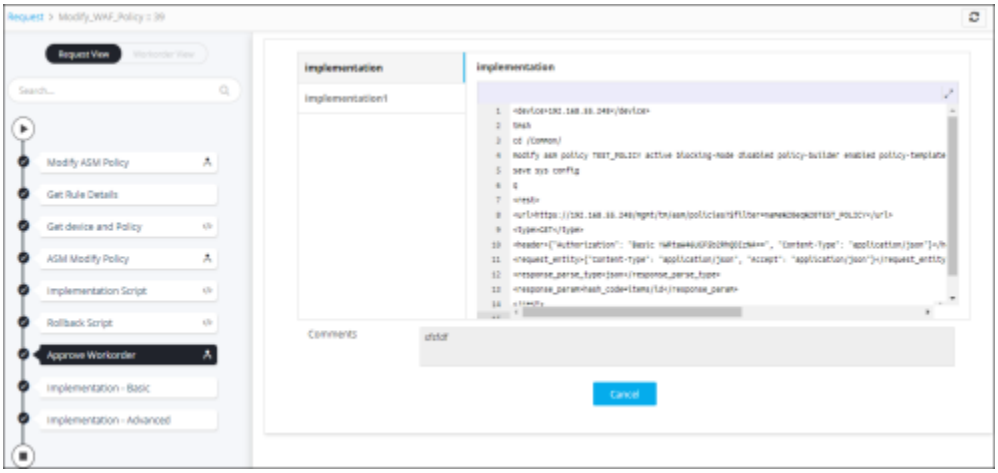

> **Note:** If the **HTTPS** and **TCP** protocols had appeared only in the secondary policy, they would have appeared as highlighted text rather than strike-through text.

## Modify a WAF Policy

To modify a WAF policy, complete the following steps:

1. Click and select Control Center.
2. Run a search.
3. On the search results screen that opens, click the **WAF** tab.
4. Right-click the policy name and select **Modify** from the dropdown list that appears.

5. Enter a search key for the policy you want to modify and then, click **Submit**.
   This will trigger the workflow and a new **Request ID** is created. To view the request details, refer to the Request Taskssection of this guide. The information regarding the policy you want to modify is fetched using API and the modify form for the corresponding policy will be displayed.
6. Make whatever changes you want to the policy by filling in the form fields designated with a * beside their names.
7. Click **Submit**.
   The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen. After you submit the request form, the configuration changes are reviewed and approved at AppViewX.
8. Enter any comments you have related to the implementation and then, click **Implement**.
   The configuration commands are implemented, resulting in modifying the rule or route in the device.




## Delete a WAF Policy

To delete a WAF policy:

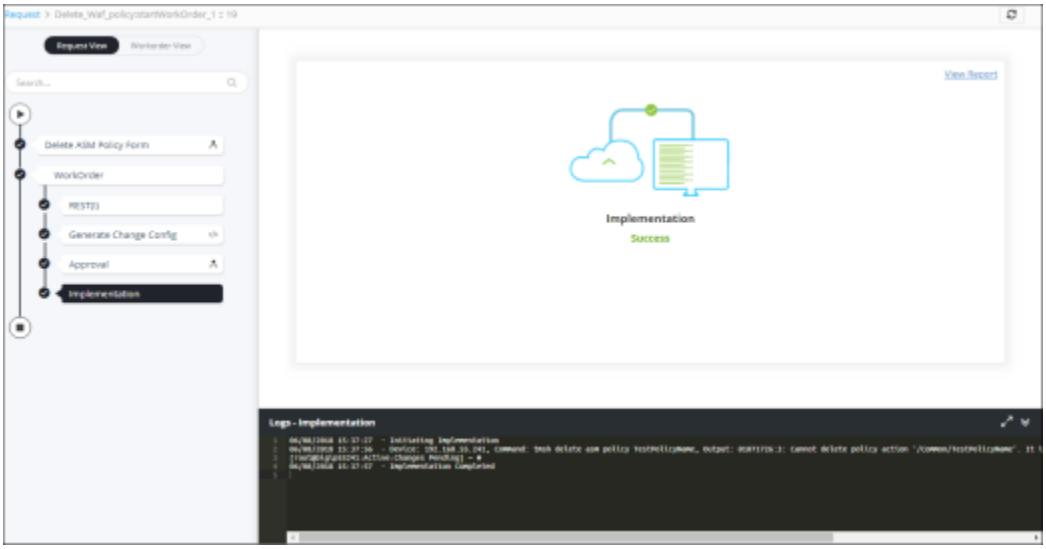
1. Click ☰ and select Control Center
2. Run a search.
3. On the search results screen that opens, click the **Firewall** tab.
4. Right-click the policy name and select **Delete** from the dropdown list that appears.
5. On the **Delete Rule** screen that pops up select one of the following actions based on how you want to trigger the workflow:

- **Confirm with CR ticket** - Creates an ITSM ticket using Service Now for tracking and approval purpose.
- **Confirm without CR ticket** - Deletes a policy without creating an ITSM ticket using Service Now for tracking and approval purpose.
- **Discard request** - Exits the Delete Rule screen.

6. Click **OK** to trigger a workflow.

   A new **Request ID** is created. To view the request details, refer to the Request Tasks section of this guide. The work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the Logs pane at the bottom of the screen. The information regarding the policy you trying to delete is fetched using API and the configuration changes are reviewed and approved at AppViewX.
7. Enter any comments you have related to the implementation and then, click **Implement**.

   The configuration commands are implemented, resulting in deleting the rule or route from the device.




## 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 and select Control Center.
2. Search for the ADC object whose actions menu you want to access.
3. In the **search results** field, 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  beside the object or  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.
- 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** - 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.
  - 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
  - The following are the additional actions that can be performed only on the topology view of the ADC device objects:
    - **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

## Access the Actions Menu for Objects Within Certificate Topologies

To access the actions menu for an object that appears within a Certificate topology:

1. Search for the certificate object whose topology you want to view.
2. Click the object's name in the search results field.
3. On the topology screen that 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, but the most common ones are listed below. To initiate any of the actions, scroll down in the list and click the corresponding action button.

   - Certificate actions
     - Download certificate
     - Upload certificate
     - Export certificate
     - Assign or unassign a group to a certificate
     - Upload key

  - Download key
  - Renew
  - Reissue
  - Regenerate
  - Revoke
  - Rollback
  - Delete certificate
- Application connector actions
  - Push to devices
  - View log
  - View alert
  - Edit
  - Delete
- Certificate Authority connector actions
  - View log
  - View alert
  - Edit
  - Delete
- Monitor connector actions
  - View log
  - View alert
  - Edit
  - Delete
- SSL template and profile actions
  - Push to device
  - View log
  - View alert
  - Disassociate from device
- Monitor actions
  - View log
  - View alert
  - Disassociate from device

## View Complete Details of a Certificate

To view all the details of a certificate in a certificate topology:

1. Open the Certificate topology containing the certificate whose details you want to view.
2. In the Certificate topology view, click the certificate. A Certificate details screen pops up, providing a complete summary of the certificate details.
3. Click any row in the table to have its contents displayed in the bottom half of the screen.


This is particularly useful for entries, like Authority information access shown in the image below, that is too long to display completely in the top half of the screen.

## Access the Actions Menu for Rules on the Firewall Search Results Screen

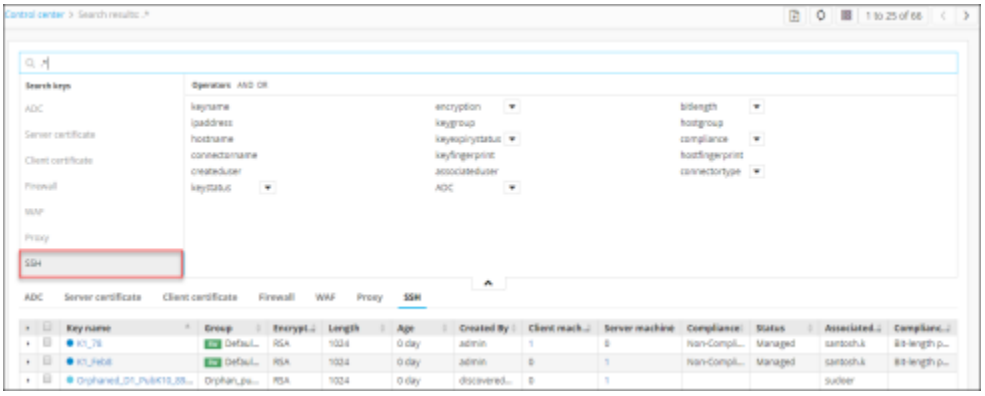
To access the actions menus for rules that appear on the Firewall search results screen:

1. Click and select Control Center.
2. Search for the Firewall rules whose actions menu you want to access.
3. In the search results field, right-click the rule or any of the other associated details to view the list of actions you can perform.
4. To initiate any of the actions, click the corresponding action button.
   - **View config** - View the current configuration of the firewall rules. For more details, refer to the View Configuration details section of this guide.
   - **View NAT rules** - View the list of NAT rules associated with the selected rule.
   - **Delete** - Delete a rule that is associated with the device.
   - When you select this option, the respective workflow opens requesting you to fill in all the form fields and click **Submit**. A new request ID will be created to delete the selected rule from the device.

# Access the Actions Menu for Keys Within SSH Holistic View

To access the actions menu for an SSH key that appears within a holistic view:

1. Search for the SSH key whose holistic view you want to view.
2. Click the SSH key name in the search results field.



3. On the holistic view screen that appears, right-click any of the components to view the list of actions you can perform.

   The actions that appear in the list vary depending on the type of component you right-click, but the most common ones are listed below:

   - Push
   - Rollback
   - Retry
   - Renew
   - Reissue
   - Regenerate
   - Rotate
   - Refresh
   - Delete
   - Download
   - Export

# Chapter 4: Appvision

- AppVision Module
- Application
- Service

## AppVision Module

AppVision is an application-centric network management platform that orchestrates and automates all the application related actions and requests across multi-vendor and hybrid infrastructure. It allows you to model, deploy, monitor, and manage the applications and their related network components on-premises.

The AppVision module is divided into two panes:

- Application
- Service

## Application

- Application Pane
- Inframap
- Discovery
- DNS Mode
- GSLB Mode
- SLB Mode
- Discover AppViewX Mode
- Custom Discovery Mode
- Workspace of an Inframap
- State and Status of the Component
- Navigation Bar
- Provision an Inframap
- View the Deployment History
- Access the Actions Menu
- View the Component Details in Inframap

- View Status Summary
- Delete a Service Component
- Troubleshoot an Inframap
- View the Troubleshoot History
- View the Monitoring Status
- Rediscover an Application Infrastructure
- Quick Sync to Refresh the Application Infrastructure
- Export an Inframap as Code
- Create a Custom View
- Grouping the Service Components
- View AppVision Component Reports
- View Action Logs
- Update an Application Infrastructure
- Blueprint
- Out of Box Support
- Create a Blueprint
- Workspace of a Blueprint
- Provision a Blueprint
- Clone as a Blueprint
- View the Component Details in Blueprint
- Import an Inframap as Code
- Edit an Inframap or Blueprint Description
- Upload a File to an Inframap or Blueprint
- Download a File from an Inframap or Blueprint
- Delete an Inframap or Blueprint

## Application Pane

The Application pane allows you to model, deploy, manage, and monitor an application infrastructure. The following tabs are available on the Application screen:

- Inframap
- Blueprint

## Inframap

A topological view of a deployed application infrastructure is displayed as an Inframap. The live application infrastructure can be enhanced by modifying the Inframap and submitting additional service requests based on the use case of application and network engineers. Also, Inframaps can be reused by network engineers to build another application by creating a backup.

## Discovery

AppVision discovers the application and its associated network components intuitively, by parsing their configurations and building Inframaps. It can map and leverage the application-centric services that are not managed at AppViewX via API(s) and represent them as part of the Inframap. The discovered Inframaps shows the connection between different service components, such as GTMs, LTMs, pools, pool members, firewalls, and so on.

The following are the quick discovery methods pre-configured in AppVision based on which the application infrastructure is discovered:

- **DNS**
- **GSLB**
- **SLB**
- **Discover AppViewX**
- **Custom Discovery**

Also, the user has a provision to create a discovery mode based on which he or she wants to discover the multi-vendor network devices.

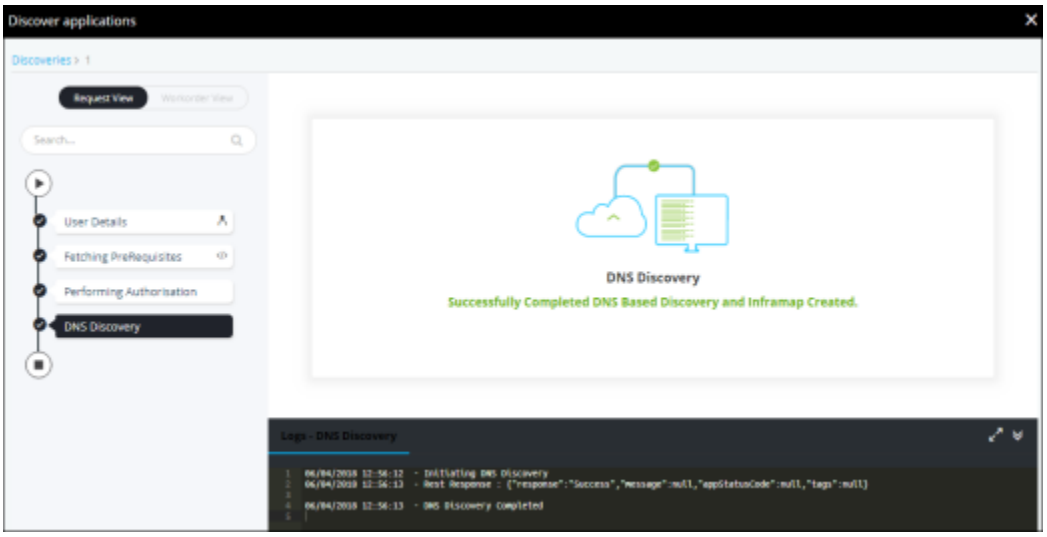
## DNS Mode

A DNS lookup is performed to resolve the DNS name of the GTM using the domain name or IP address of an application. An Inframap is created after successful completion of discovering the following objects:

- The Wide IPs, virtual servers, end servers, pools, and pool members associated with the application are retrieved from the database.
- The virtual server retrieves the certificate details using profiles.
- The virtual IP address retrieves the NAT rules, ingress, and egress security policies associated with the source and destination IP port.
- The pool member IP address retrieves the certificate details, NAT rules, ingress, and egress firewall security policies at the end server level.

To discover an application infrastructure based on DNS:

1. Click ☰ and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click Discover X in the command bar.
   The **Discovery** screen that pops up displays all the pre-configured quick discovery modes.
3. Click ▶ beside the DNS discovery mode.
4. On the request form, enter a name or IP address for the application or a URL to discover the modules associated with the application.
5. In the Port field, enter the port number for the application you want to discover.
6. Click **Discover** to trigger the discovery.
7. A new **Request ID** is created. The request details along with their status are displayed in the **Discovery status** tab.
8. Click the **Request ID** to view the work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details.
   Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.




## GSLB Mode

A GSLB discovery is performed using the GSLB servers/Wide IP(s) that are parsed after the device addition in AppViewX inventory. An Inframap is created after successful completion of discovering the following objects:

- The virtual servers, end servers, pools, and pool members associated with the device are retrieved from the database.
- The virtual server retrieves the certificate details using profiles.
- The virtual IP address retrieves the NAT rules, ingress, and egress security policies associated with the source and destination IP port.
- The pool member IP address retrieves the certificate details, NAT rules, ingress, and egress firewall security policies at the end server level.

To discover an application infrastructure based on GSLB:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click 

in the command bar.
   The *Discovery* screen that pops up displays all the pre-configured quick discovery modes.
3. Click  beside the GSLB discovery mode.
4. Select the **Yes** or **No** radio button depending on whether you want to discover all the **GSLB/BIG-IP DNS** associated with the devices that are managed in AppViewX. Skip to step 7. to build the Inframaps.
5. To discover the GSLB/BIG-IP DNS of a specific device, click **No** in step 5 and do the following:
   a. In the **Device** dropdown field, select the device whose objects you want to fetch from the database.
   b. In the **GSLB Servers / Wide IP** dropdown field, select the GSLB server or wide IP for which you want to build an Inframap.
   c. Click  .
   The device and GSLB server details are displayed in the **GSLB/BIG-IP DNS** table at the bottom of the screen. You can delete or modify the details by selecting the checkbox beside the troubleshooting options in the table at the bottom of the screen and then clicking either  or  .
6. Click **Discover** to trigger the discovery.
   A new **Request ID** is created. The request details along with their status are displayed in the **Discovery status** tab.

7. Click the **Request ID** to view the work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details.
   Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.

## SLB Mode

A reverse lookup is performed using the SLB/Virtual Servers that are parsed after the device addition in AppViewX inventory. An Inframap is created using the hostname after successful completion of discovering the following objects:

- The virtual server pools and pool members associated with the device are retrieved from the database.
- The virtual server retrieves the certificate details using profiles.
- The virtual IP address retrieves the NAT rules, ingress, and egress security policies associated with the source and destination IP port.
- The pool member IP address retrieves the certificate details, NAT rules, ingress, and egress firewall security policies at the end server level.

To discover an application infrastructure based on SLB:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click 

in the command bar. The *Discovery* screen that pops up displays all the pre-configured quick discovery modes.
3. Click  beside the SLB discovery mode.
4. Select the **Yes** or **No** radio button depending on whether you want to discover all the **SLB/Virtual Servers** associated with the devices that are managed in AppViewX. Skip to step 7. to build the Inframaps.
5. To discover the SLB/Virtual Servers of a specific device, click **No** in step 5 and do the following:
   a. In the **Device** dropdown field, select the device whose objects you want to fetch from the database.
   b. In the **SLB/Virtual Servers** dropdown field, select the SLB server or virtual server for which you want to build an Inframap.
   c. Click  .
   d. The device and SLB/Virtual server details are displayed in the **SLB/Virtual Servers** table at the bottom of the screen. You can delete or modify the details by selecting the checkbox beside the

troubleshooting options in the table at the bottom of the screen and then clicking either  or  .

e.

6. Click **Discover** to trigger the discovery.
   A new **Request ID** is created. The request details along with their status are displayed in the **Discovery status** tab.
7. Click the **Request ID** to view the work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details. Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.

## Discover AppViewX Mode

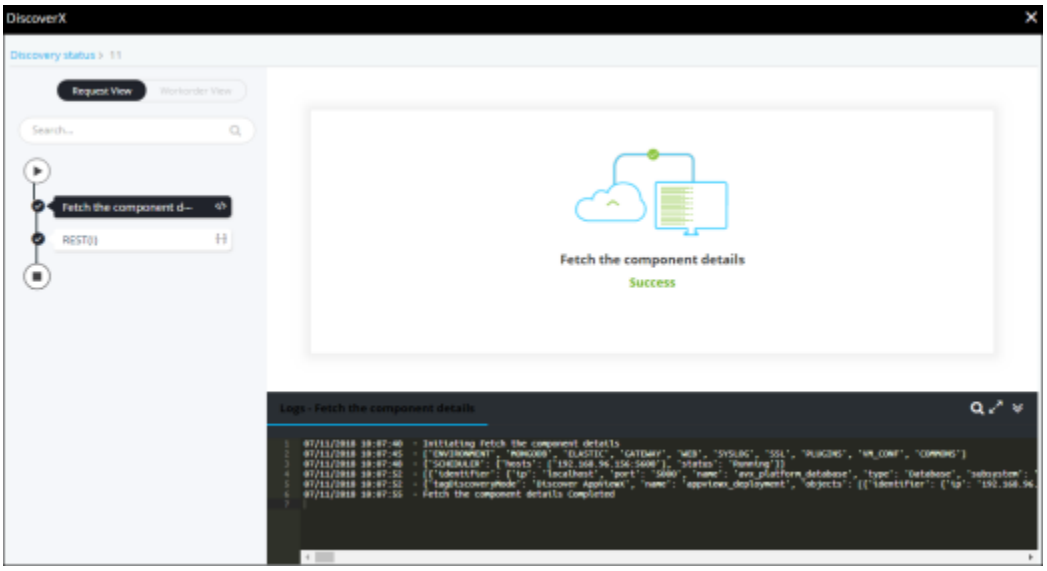
Discover AppViewX mode enables the user to discover AppViewX as an application along with its logical components such as web server, gateway, logstash, elastic search, service plugins, and database.

To discover AppViewX as an application:

1. Click  and select **AppVision** > **Application**.
2. The **Application** screen opens with the **Inframap** tab selected by default.
3. Click 

in the command bar. The *Discovery* screen that pops up displays all the pre-configured quick discovery modes.
4. Click  beside the Discover AppViewX mode.
5. On the pop-up screen that opens, click **OK** to create a request.
6. A new **Request ID** is created. The request details along with their status are displayed in the **Discovery status** tab.
7. Click the **Request ID** to view the work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details.

Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.



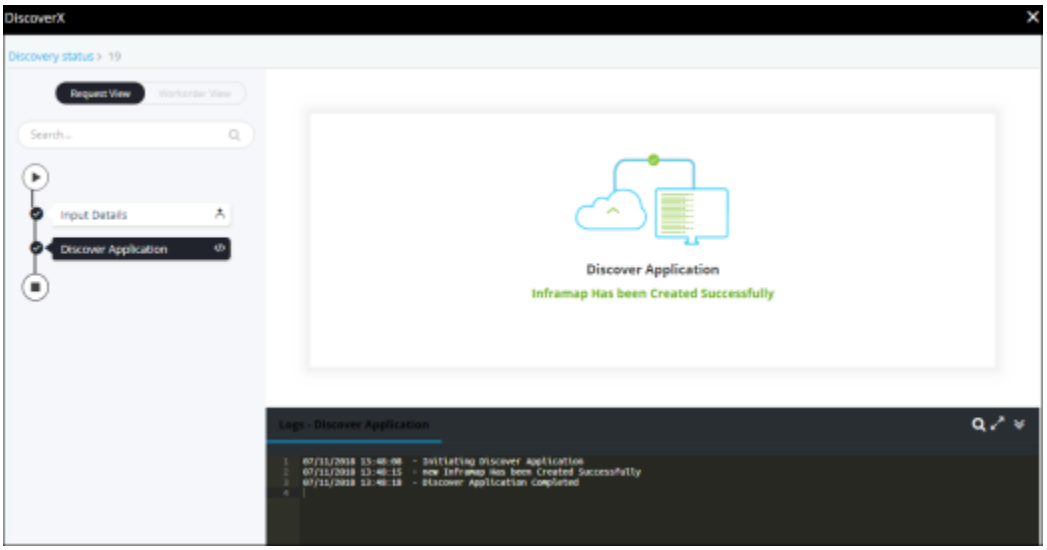

## Custom Discovery Mode

The Custom discovery mode enables the user to customize the discovery of applications and their associated load balancers, certificates, and firewalls.

To customize the discovery of an application:

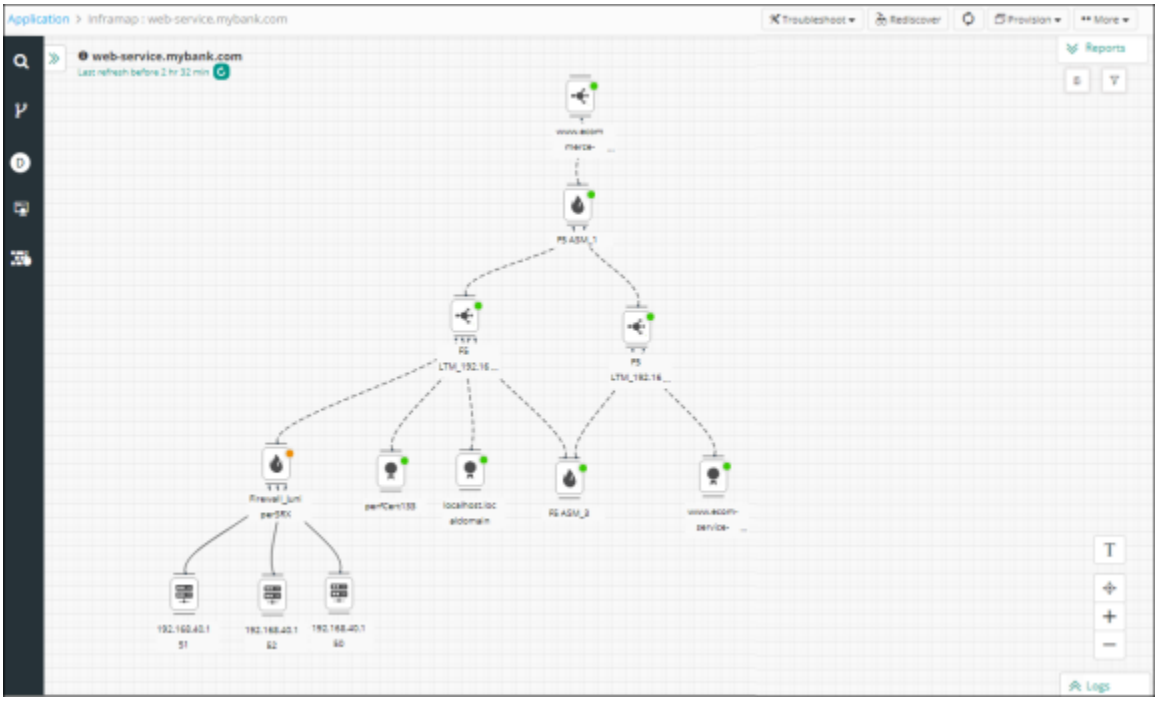
1. Click ☰ and select **AppVision** > **Application**.
2. The **Application** screen opens with the **Inframap** tab selected by default.
3. Click Discover X in the command bar. The **Discovery** screen that pops up displays all the pre-configured quick discovery modes.
4. Click ▶ beside the Custom Discovery mode.
5. At a minimum fill in all fields that contain a * beside their names.
6. Click **Discover** to trigger the discovery.
7. A new **Request ID** is created. The request details along with their status are displayed in the **Discovery status** tab.
8. Click the **Request ID** to view the work order tasks or phases of the corresponding request are listed in a tree-view. You can click each task to view its details.

Wherever applicable, all the logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.




## Workspace of an Inframap

A workspace of an Inframap provides complete application-centric visibility by representing a live application infrastructure intuitively with the state, status and topology view of the managed service components.



The workspace view allows you to view and perform the following tasks:

- View the State and Status
- Navigation Bar
- Access the Actions Menu
- View Component Details
- Delete a Service Component
- Troubleshoot an Inframap
- View the Troubleshooting history
- View the Monitoring status
- Rediscover an Application Infrastructure
- Quick Sync an Application Infrastructure
- Provision
- History
- Clone as Blueprint
- Export
- Create a Custom View
- Grouping the service components
- View AppVision Component Reports
- View Action Logs

## State and Status of the Component

AppVision has a provision to display the state and statuses of a service component in the live application. This enables network engineers to troubleshoot the application infrastructure rapidly.

The following color codes are used to identify the statuses of each component in the workspace view:

**ADC**

- Green - All the objects in a device are enabled.
- Red - All the objects in a device are disabled.
- Orange - Combination of both enabled and disabled objects in a device.

**Certificate**

- Green - Certificate is available and valid.
- Red - Certificate has expired.
- Orange - Combination of both valid and expired certificates.

**Firewall**

- Green - Rule is valid.
- Red - Rule is not valid.
- Orange - Combination of both.

## Navigation Bar

The service components that are configured and published in the **Service** section are grouped under the navigation bar.

To go to the navigation bar:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure that you want to modify from the Inframap screen.
3. You can type the name of the application infrastructure in the search box to find it. Using the **All** dropdown, you can select the type of search (**All**, **Mode**, or **Device**) you want to perform.
4. On the navigation bar that appears at the left corner of the workspace, select one of the following tabs.
   -  **ADC**
   -  **Default**
   -  **Certificate**
   -  **Firewall**
5. Upon expanding, you can drag and drop the required service components to the workspace.
6. Click  or  and enter the name of the component you want to search by in the search field.

## Provision an Inframap

Provisioning the live application infrastructure in AppVision enables the user to:

- Add some additional components to the already discovered or built Inframaps.
- Globally deploy those components/Inframaps in the Hybrid environment.

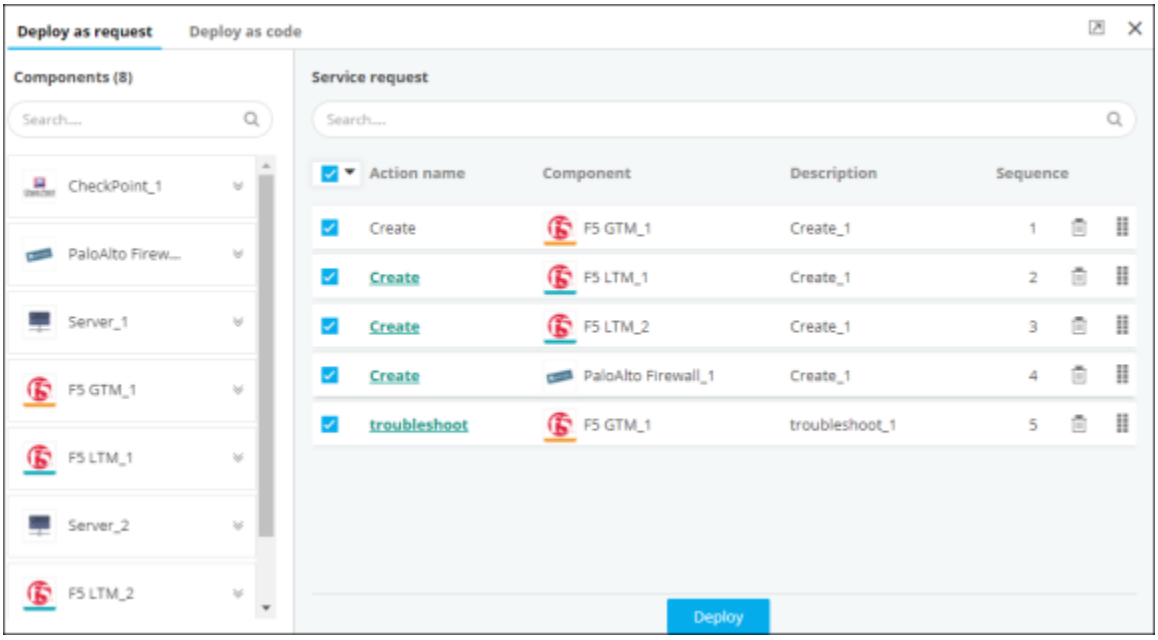
You can deploy an Inframap using one of the following methods:

- Deploy as Request
- Deploy as Code

## Deploy as Request

To deploy an Inframap using the service requests:

1. Click and select **Menu** > **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure and make whatever changes are required.
3. Click the **Provision** dropdown menu and select Provision in the Command bar.
   An **Alert Message** screen will pop up asking you to take a backup of the application before deploying any changes. Enter a name for the **Blueprint** to help the users identify it.
4. Click the **Save** button.
   A copy of the live application infrastructure is created and the deployment screen opens with the **Deploy as request** tab selected by default.




5. A list of available components that are used in designing the application is displayed under the **Components** section.
6. Click each service component.
   The field expands to display a list of actions associated with the service component.
7. Drag and drop the workflows to the *Service requests* section.

8. Click  to arrange the requests in the sequence that you want the automation tasks to be executed. Also, you can delete the requests from the request cart by clicking  .
9. Select the workflow and on the respective *Request form* screen that opens, fill in all the fields that contain a * beside their names.
10. Click **Save draft** to save a draft of the workflow.
11. Repeat Steps 9 and 10 for all the workflows.
12. Click the **Deploy** button. The service requests are then deployed in the sequence you designated in the Request cart.
    A popup message is displayed at the top of the workspace: **Application deployment request submitted**. The changes made to the live Inframap are deployed only when the deployment request starts to retrieve the objects. The pre-validation and post validation scripts help the user ensure that the deployment was successful.

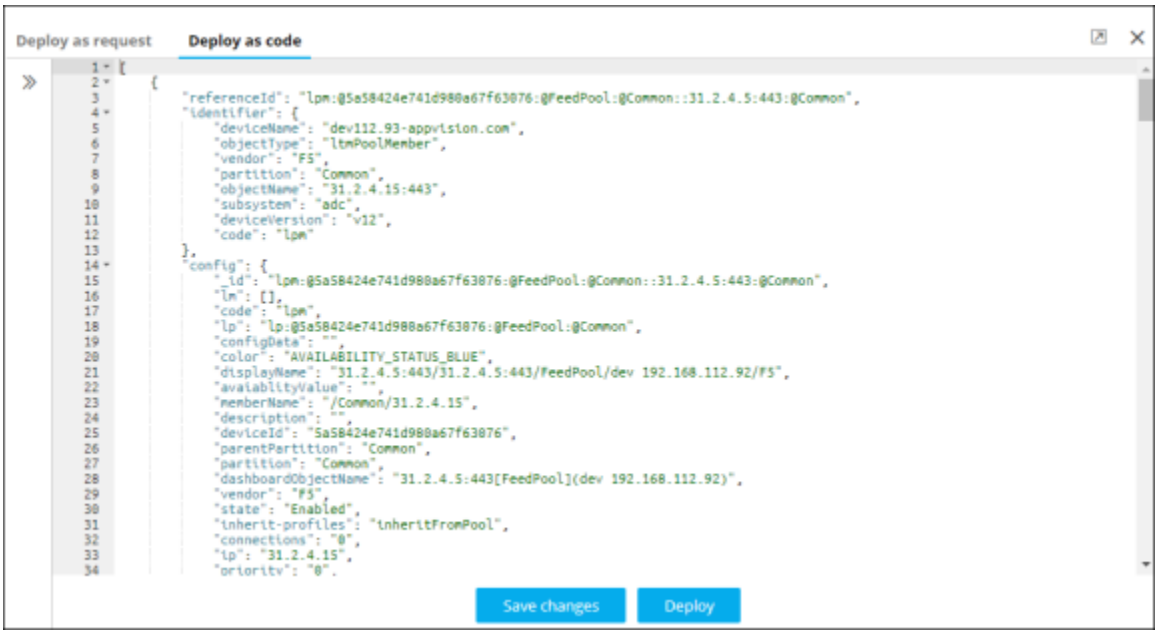
## Deploy as Code

To deploy an Inframap as a code, complete the following steps:

1. Click  and select **Menu** > **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure and make whatever changes are required.
3. Click the **Provision** dropdown menu and select 

in the Command bar.
   An **Alert Message** screen will pop up asking you to take a backup of the application before deploying any changes. Enter a name for the **Blueprint** to help the users identify it.
4. Enter a name for the **Blueprint** to help the users identify it.
5. Click the **Save** button.
   A copy of the live application infrastructure is created and the deployment screen opens with **Deploy as request** tab selected by default.
6. Click the **Deploy as Code** tab.
7. Copy and paste the code file of the application infrastructure that you have saved on your computer.

8. Click **Save changes** to save the file, which can be deployed later, or click **Deploy** to deploy the changes immediately.




## View the Deployment History

The Deployment history feature provides a chronological summary for each Inframap or Blueprint based on how you deployed them.

- Workflow
- Infra as Code

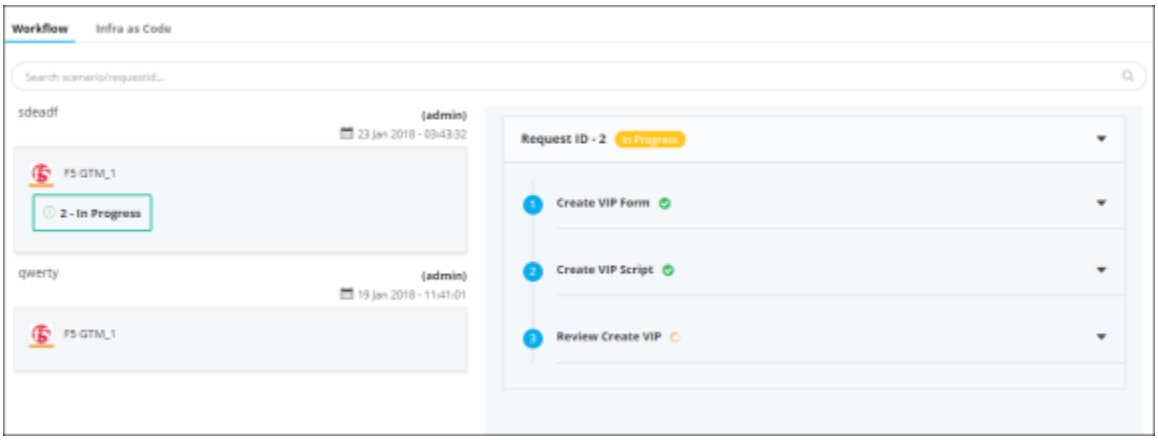
## Workflow

To view the deployment history details for the Inframaps or Blueprints that are deployed using the service requests:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to view the deployment history of a Blueprint, select the application from the **Blueprint** tab and do the following.
3. Open the application whose history you want to review.
4. On the workspace that opens, click the **Provision** dropdown menu and select History in the Command bar.

The deployment history screen opens with the **Workflow** tab selected by default. A summary of scenario-based deployments, requests, and logs for each Inframap is displayed.

5. Click  to view the details of each task.



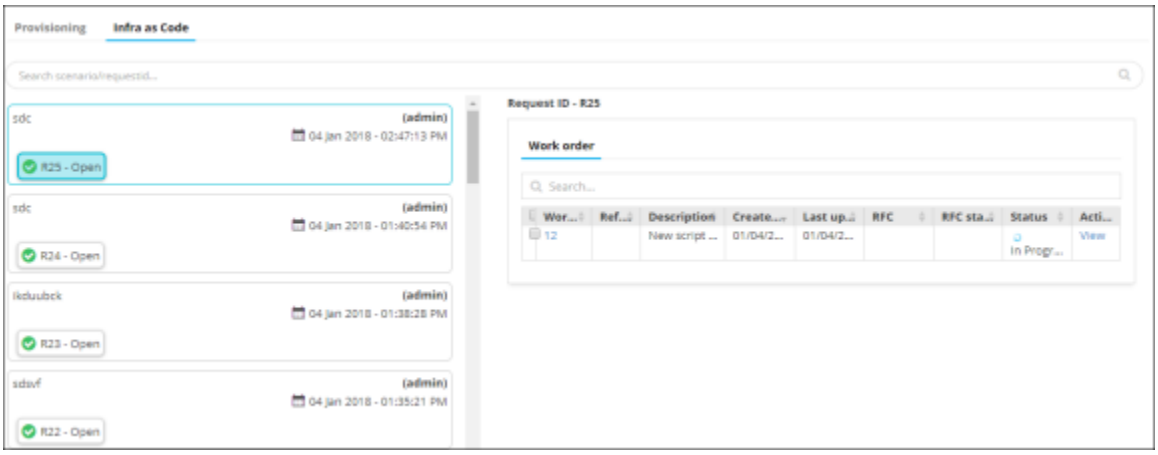

## Infra as Code

To view the deployment history details for the Inframaps or Blueprints that are deployed as a code:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to view the deployment history of a Blueprint, select the application from the **Blueprint** tab and do the following. Open the application whose history you want to review. On the workspace that opens, click the **Provision** dropdown menu and select 

in the Command bar. The deployment history screen opens with the **Workflow** tab selected by default.
3. Click the **Infra as Code** tab.

A summary of requests and work order details for each Inframap is displayed. Click the **View** link in the **Activity** column to view the work order summary in a stage view.




## Access the Actions Menu

The automation service requests associated with the service components in **Service** pane are implemented using workflows. This feature allows the user to trigger an automation task on a specific application infrastructure component.

To run the workflows in your environment, ensure that the following prerequisites are met:

- Workflows and Helper scripts are imported to your environment.
- Workflows are enabled in the APS/Orchestrator engine.
- You have the required access permissions to view and submit service requests for deployment.

To access the Actions menu:

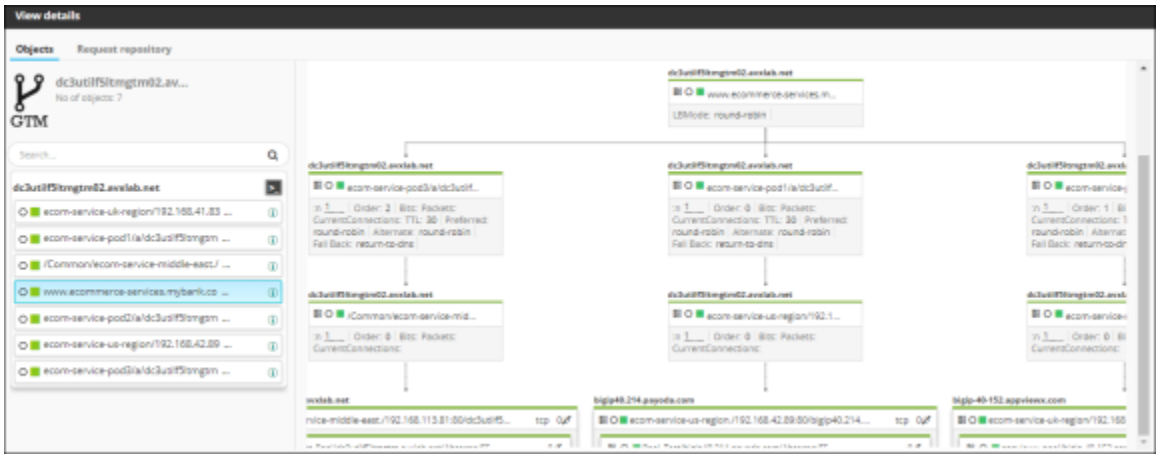
1. Click  and select **AppVision** > **Application**.
   The Application screen opens with the **Inframap** tab selected by default.
2. Click the Inframap on which you want to make changes.
3. If you want to invoke an automation service request to any component that appears in a Blueprint, select the application infrastructure from the **Blueprint** tab and on the workspace that opens, right-click the service component and select **Actions**.
   All automation service requests associated with the component are listed.
4. Select the workflow. (Only applicable for Inframaps)
   An Alert message screen pops up asking you to take a backup of the application before making any changes to the live Inframap.
5. On the respective **Request Form** that opens, fill in all the mandatory fields.

6. Click **Save Draft** to save a draft of the workflow, which can be submitted later or click **Submit** to trigger the action immediately.
   A pop-up message appears at the top of the workspace, ***Request ID** is created.*
7. To view the request details, refer to the View Component Detailssection.

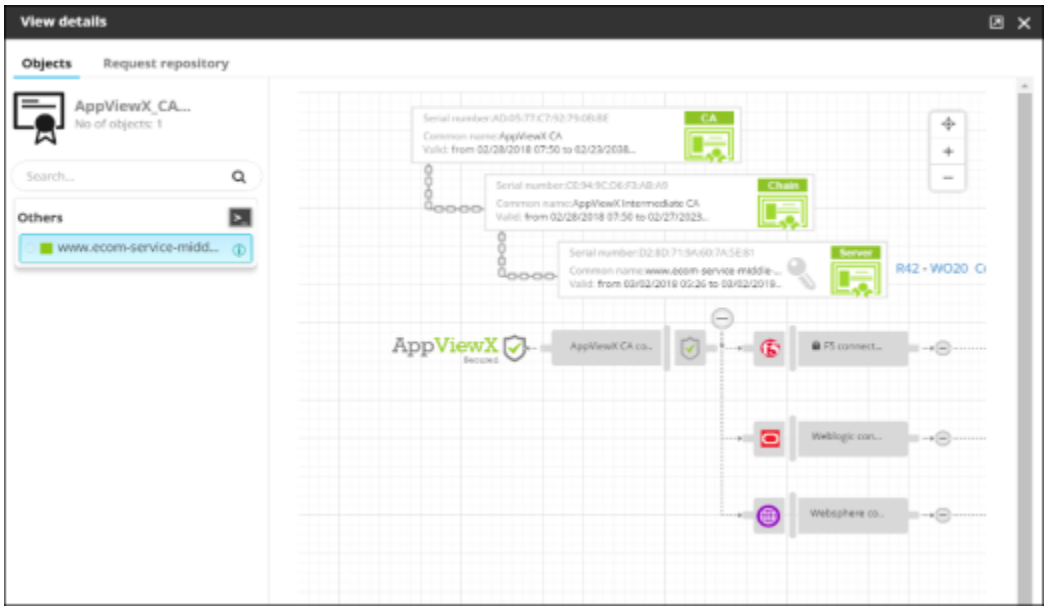
## View the Component Details in Inframap

To view the details of any component that appears in the live application infrastructure:

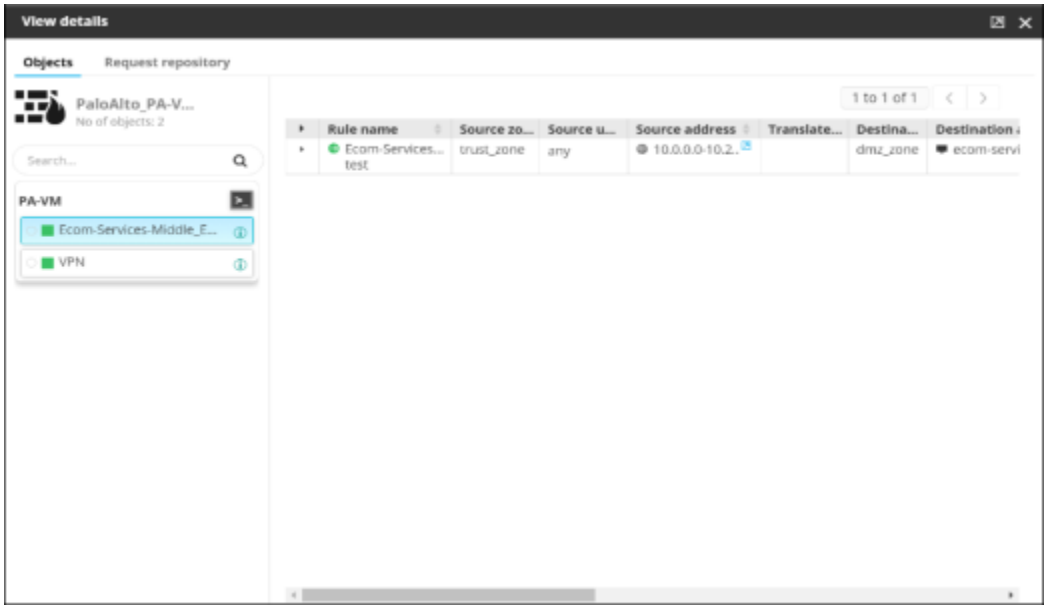
1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the Inframap whose component details you want to view.
3. If you want to view the details of a component that appears in a Blueprint, select the application from the Blueprint tab and do the following.
4. On the workspace that opens, right-click the component and select **Details**.
   The **Details** screen opens with the **Objects** tab selected by default. The list of objects appears varies depending on the component type you selected.
   - **ADC:** A topology view for each device object provides a detailed, hierarchical map of the structure of the object and their dependencies.




   - **Certificate:** The topology view for each certificate provides a detailed map that extends from the root certificate to intermediate certificates to the end certificate itself. This view also shows the relationship between all of the other components related to the certificate, including connectors and devices.




- **Firewall:** The detailed information about the rules and policies available within the selected component is displayed.

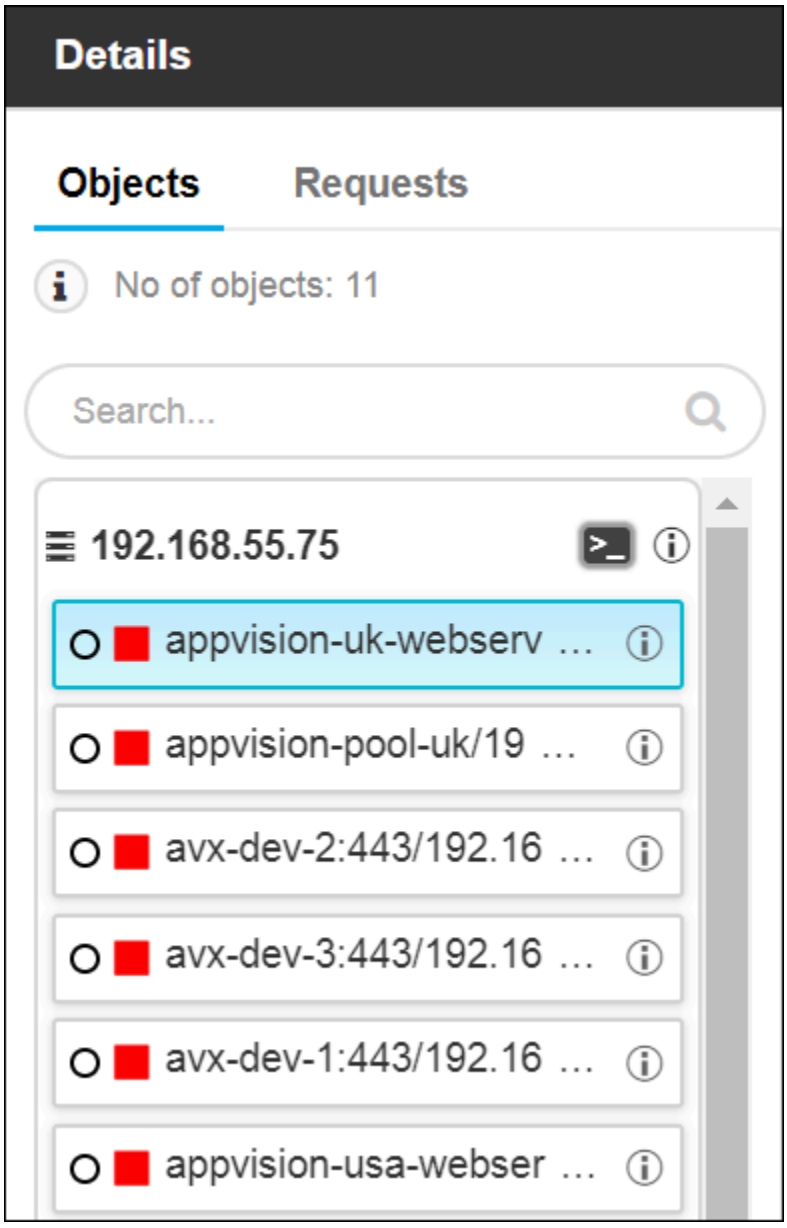



5. You can right-click the object to view the list of actions that can be performed.

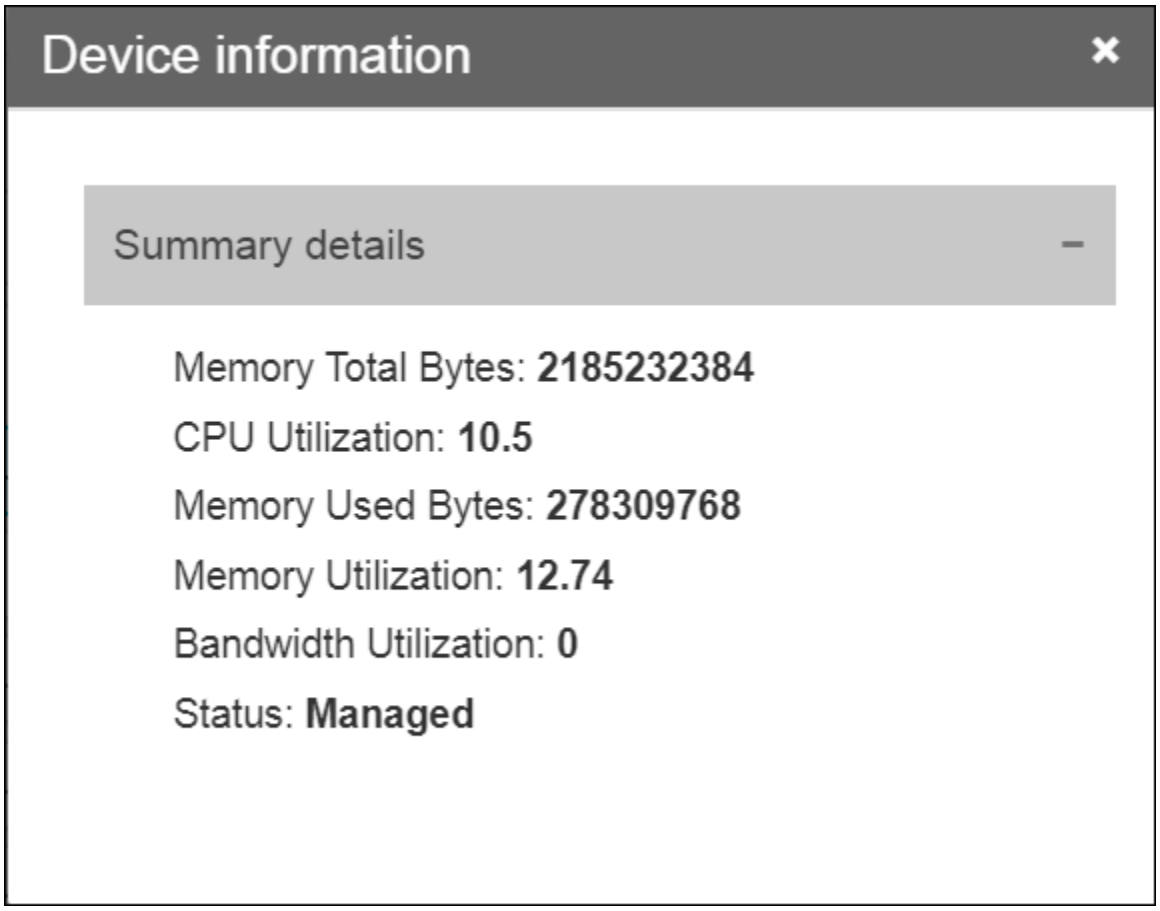
   For more details, refer to the following:

   - ADC - Access the Actions Menu for Objects on the ADC Search Results and Topology Screens
   - Certificate - Access the Actions Menu for Objects Within Certificate Topologies
   - Firewall - Access the Actions Menu for Rules on the Firewall Search Results Screen
   - Right-click an object and select the **Details** option.

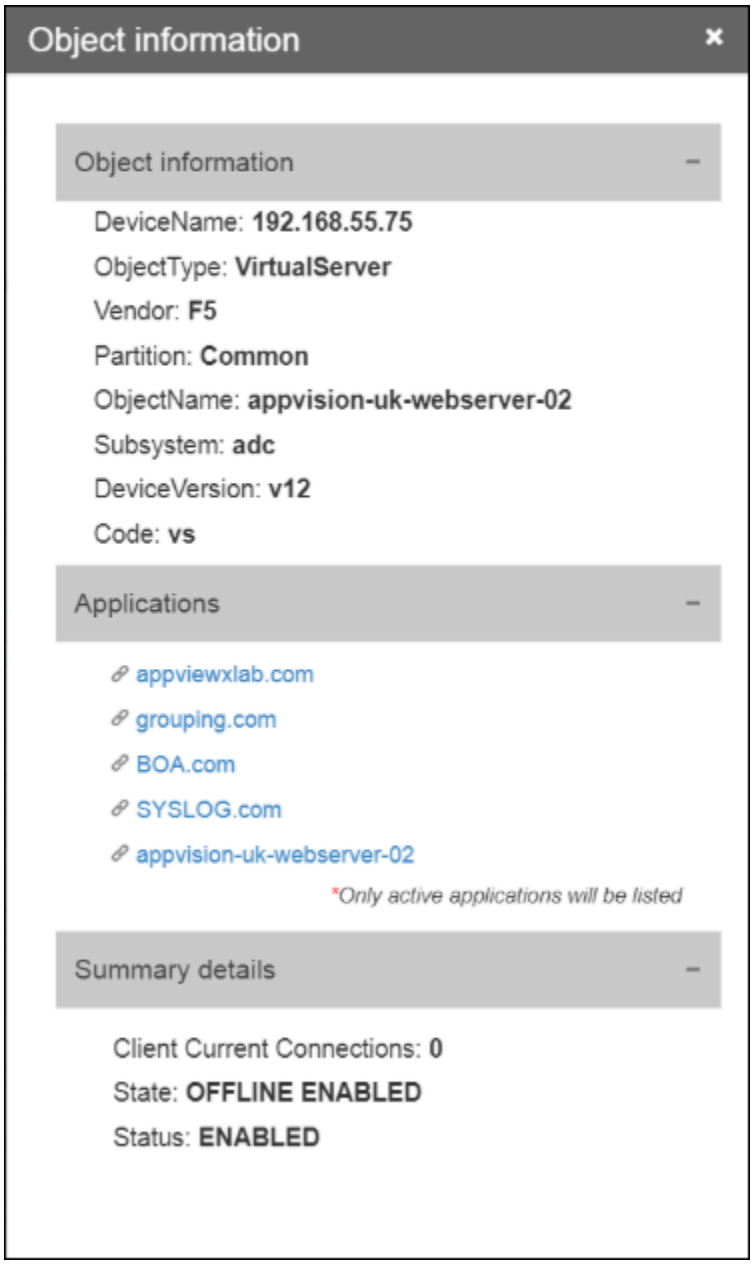
- In the **Details** screen that appears, all the object details are displayed on the left side in the **Objects** tab.




- Click ⓘ to view the advanced health monitor containing the statistics of CPU usage.



- Click ⓘ to view the cross-functional application details.

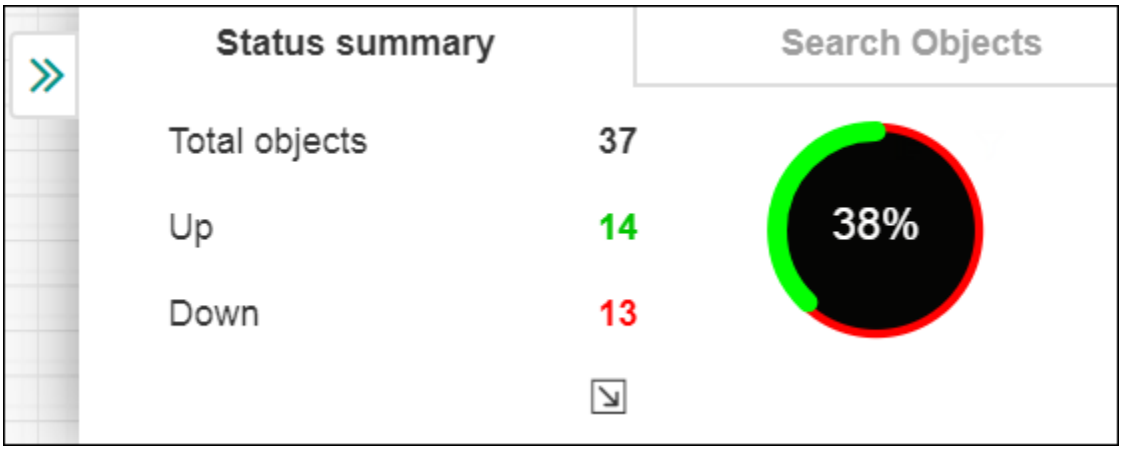



## View Status Summary

To view the status summary of an application in AppVision module:

1. Click ☰ and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.

2. Open the application whose status summary wants to view.
3. On the workspace that opens, click  .
   The status summary appears at the right side of the screen as shown below:




4. You can click  to view the device and object details. Also, you can click on the **Search Objects** tab to search for any device objects of your choice.

## Delete a Service Component

To delete any component that appears in the application infrastructure:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application from which you want to delete a service component.
3. If you want to delete a component that appears in a Blueprint, select the application from the Blueprint tab and do the following.
   a. You can delete only the additional components that are added to the Inframap.
   b. The component that has objects in it cannot be deleted from the Inframap.
   c. On the workspace that opens, right-click the service component and select **Delete**.
   d. On the **Confirmation** screen that pops up, click **Yes**.

## Troubleshoot an Inframap

The one-touch troubleshooting and monitoring method in AppVision enables the network engineers to identify and remediate network issues (such as CPU spike, firewall port block, or ping checks) at a device or object level. The following are the actions that are performed as part of troubleshooting:

## Configure

The Troubleshoot utility is configured and defined for an application using the CLI commands, scripts, and custom monitors. This allows the user to perform a connectivity check from one endpoint (Source IP) to another endpoint (Destination IP) across all the components of an application.

Before configuring the troubleshooting method, ensure that the following prerequisites are met:

- Workflows and Helper scripts are imported to your environment.
- Workflows are enabled in the APS/Orchestrator engine.
- You have the required access permissions to view and submit the requests for deployment.

To configure:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure that you want to troubleshoot.
3. Click the **Troubleshoot** dropdown menu and select 

in the Command bar.
4. On the *Troubleshoot* screen that opens, all the service components associated with the application are listed on the left side of the screen.
5. Select the checkbox beside the component name.
6. If you have the command and string for the component that you want to troubleshoot, do the following:

   a. Click the **Commands** tab if it is not selected already.

   b. Select a device from the **Device name** dropdown list.

   c. Enter the CLI command and the string that must be the success criteria of command output in their respective fields.

   d. Click **Add**.
   The CLI commands and its respective match string is displayed in the table at the bottom of the screen. You can add multiple troubleshooting commands for each component.

   e. To modify or delete the details, click either  or  beside each troubleshooting suite.

7. If you want to generate a command for the component that you want to troubleshoot, do the following:

> **Note: AppViewX ||N/A||N/A** has been added in the **Source Device Name** list to enable the user to check the connectivity between the devices and AppViewX CLI.

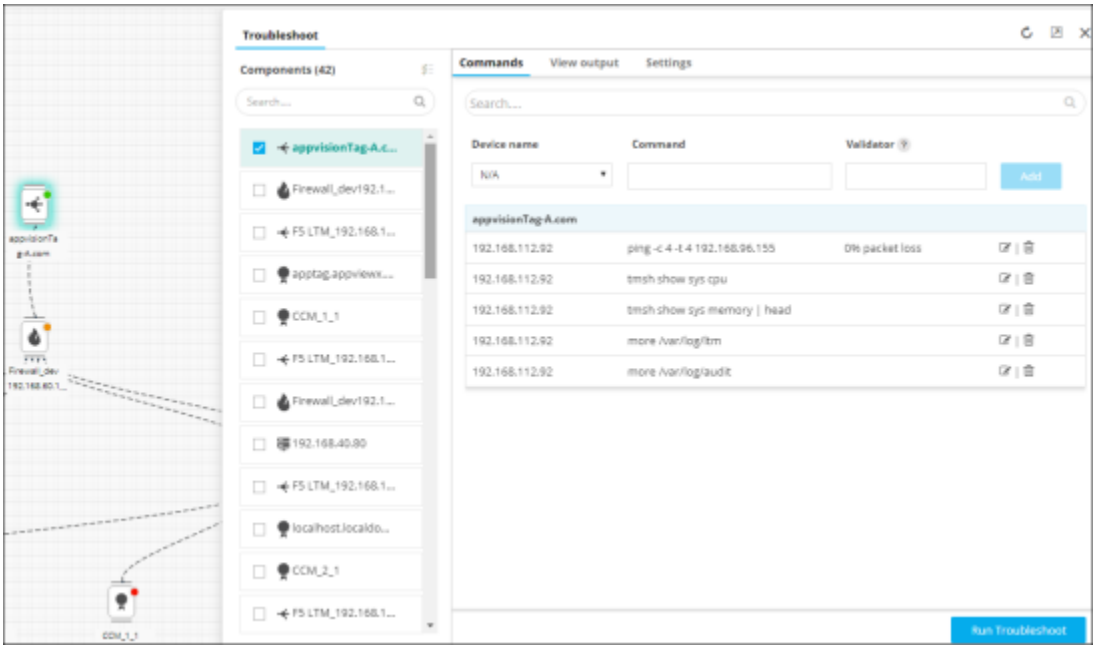
a. Click the **Settings** tab.
b. The name of the Inframap and component will automatically populate in their respective fields based on what you selected in step 5.
c. Select the **Device** or **Object** radio button depending on how you want to monitor the service component.
d. Under the **Generate Commands** sections, select the troubleshooting option for which you want to generate a monitoring command.
e. In the **Description** field, click  to fetch the information about the troubleshooting option you selected in Step 7.d. This helps the user to tell at a glance what it does.
f. In the **Source IP** field, click  to fetch the list of the source IP addresses associated with the device and select the one for which you want to check the connectivity.
g. Select the required destination IP address from the dropdown list.
h. (Only for Object Level monitoring type) Click  to fetch the list of objects associated with the device. Select the object from the dropdown list.
i. Enter the IP address of the device. The **IPv6** field will appear only if you have selected the Troubleshooting option as **PING6** or **TRACEROUTE6** in Step 7.d.
j. Enter the port number of the application. The **Port** field will appear only if you have selected the Troubleshooting option as **TRACEPATH**, **NETCAT**, or **TELNET** in Step 7.d.
k. Enter the type of record (such as A, PTR, CNAME, and so on) for the selected device. The **Record Type** field will appear only if you have selected the Troubleshooting option as **NSLOOKUP** in Step 7.d.
l. Enter the object ID for the selected object to identify its associated device and statuses. The **OID** field will appear only if you have selected the Troubleshooting option as **SNMPWALK** in Step 7.d.
m. Enter the protocol for the device. The **HTTP/HTTPS** field will appear only if you have selected the Troubleshooting option as **CURL** in Step 7.d.
n. Click  .
o. The device and object details are displayed in a **Device Details** table at the bottom of the screen. You can delete or modify the device and object details by selecting the checkbox beside the troubleshooting options and then click either  or  .

p. Click the **Generate Commands** button to generate a monitoring command for the troubleshooting option you selected in Step 7.d.
q. The device name, CLI command, and match string are generated and displayed in the **Commands to execute** the table at the bottom of the screen.
r. You can delete or modify the device name, commands, or match string by selecting the checkbox beside the device name in the table at the bottom of the screen and then clicking either  or  .
s. Click **Submit**.
t. On the **Confirmation** screen that pops up click **Yes**.

## Execute

To execute:

1. Click the **Commands** tab to review all the CLI commands.
2. Click the **Run Troubleshoot** button to implement the commands that you configured.




## View Output

You can view and analyze the command output by clicking the **View Output** tab.

- If the output of the monitoring commands contains the phrase from Match String, the following message is displayed: *Success*.
- The components that are monitored successfully will be displayed with  in the workspace.
- If the output of the monitoring commands does not contain the phrase from the Match String, the following message is displayed: **Failed**.
- The components that are failed to monitor will be displayed with  in the workspace.

**Note:** You can also troubleshoot and analyze the output of any component in the live Inframap by right-clicking it from the workspace and selecting **Troubleshoot >> Execute** or **View Output** from the dropdown menu that appears.

## View the Troubleshoot History

To view the troubleshooting history:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure for which you want to view the troubleshooting history.
3. Click the **Troubleshoot** dropdown menu and select 

in the Command bar.
   The recently executed monitoring commands along with its output will be displayed.

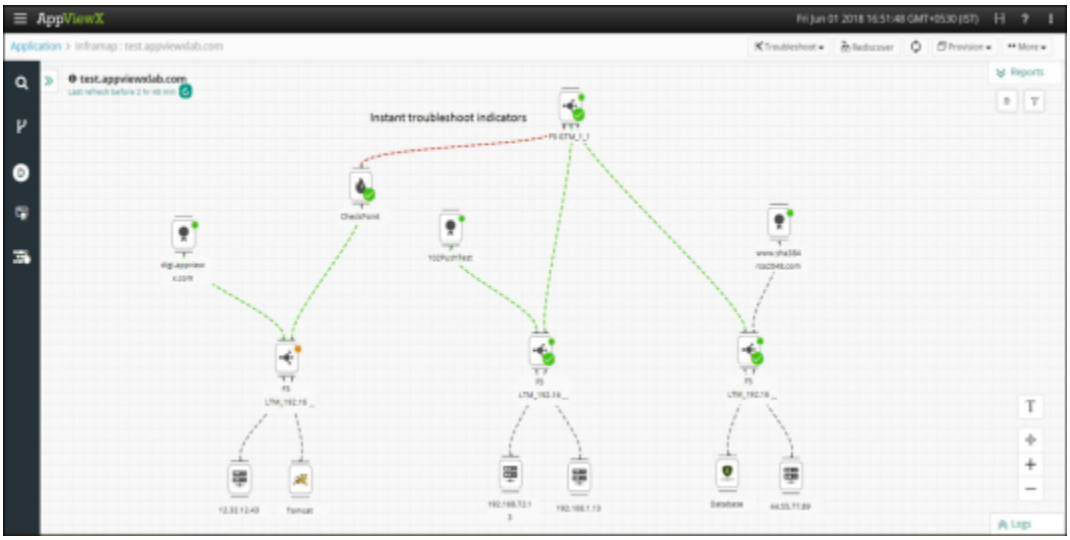
## View the Monitoring Status

To view the monitoring status:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure for which you want to view the troubleshooting history.
3. Click the **Troubleshoot** dropdown menu and select 

in the Command bar.

The Troubleshoot indicators will display the monitoring status of all the components in the workspace, for which the commands are executed.




## Rediscover an Application Infrastructure

To rediscover an application infrastructure:

1. Click ☰ and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the Inframap that you want to update. The workspace of the respective application opens.
3. Click Rediscover in the Command bar to fetch the object details from the database and update the live Inframap.
4. The Infrastructure discovery is triggered and you must refresh the screen to view the updated object details.For more details, refer to the Quick Sync to refresh the Application Infrastructuresection of this guide.

## Quick Sync to Refresh the Application Infrastructure

To refresh the application:

1. Click ☰ and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the Application that you want to refresh.
   The workspace of the respective application opens.

3. Click  in the command bar to refresh the components that appear in the workspace.
4. You can also refresh the Inframap by clicking  beside the application name in the workspace. This will refresh and update the status of all the components.

## Export an Inframap as Code

AppVision has an option to export an Inframap as code, which helps network engineers automatically manage and provision the application infrastructure.

To export an Inframap as code:

1. Click  and select **AppVision** > **Application**.
   The Application screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure whose code you want to export.
   The respective workspace opens.
3. Click the **More** dropdown menu and select 

in the Command bar.
   The selected Inframap is downloaded to your computer as a code file.
4. Select the file and navigate to the location where you want the file to go, then click **Save**.

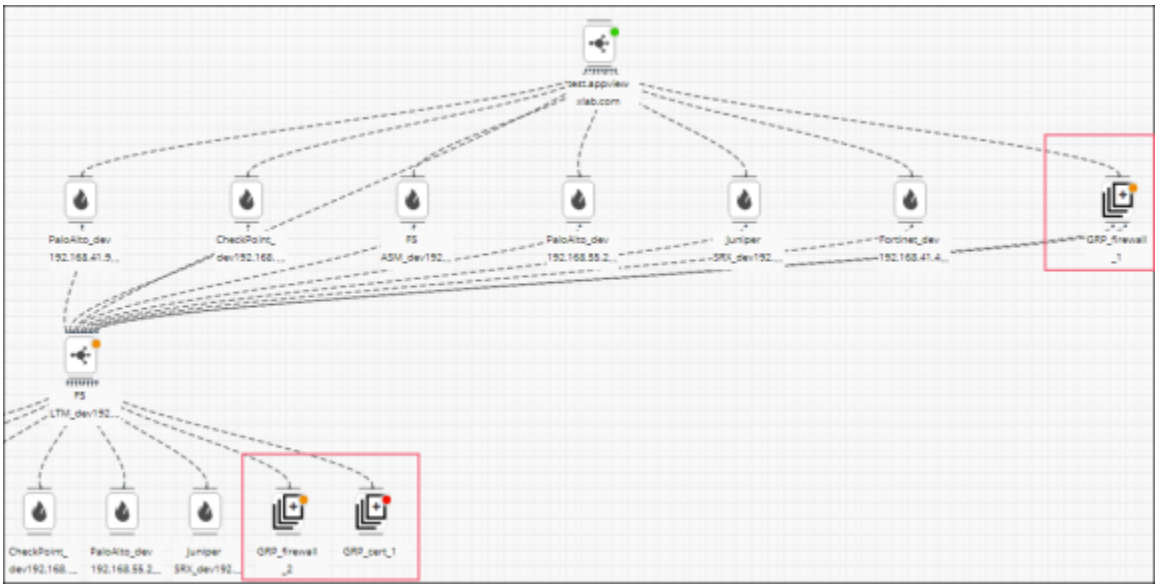
## Create a Custom View

The **Views** option in the workspace enables the user to create a customized view of a live Inframap based on the default grouping of the service components. For detailed information about the available groups, refer to the Grouping the Service components section of this guide.

To create a custom view:

1. Click  and select **AppVision** > **Application**.
   The Application screen opens with the **Inframap** tab selected by default.
2. Open the application for which you want to customize the view.
3. Click  on the right top corner of the workspace screen.
4. On the **Custom Views** pop up screen that opens, click the **Create view** button.
5. Enter a name for the view to help the users identify it. Select the radio button beside the group name based on how you want the service components to be grouped and displayed in the workspace.
6. Click **Create**.

7. Click on the newly created custom view and the service components will be displayed as shown in the following image.



8. Hover the mouse and click on the grouped elements in the workspace for a detailed view of the grouped components.

## Grouping the Service Components

All the service components are organized into various groups based on the metadata value.

To view the grouping information:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application infrastructure whose grouping information you want to view.
3. Click on the right top corner of the workspace screen.
   The following sections in the Grouping pane are used only to segregate the AppViewX components:
   - Type
   - Category
   - Node

   The following sections in the Grouping pane are used only to segregate all the Applications:
   - Device
   - Subsystem
   - Certificate Authority

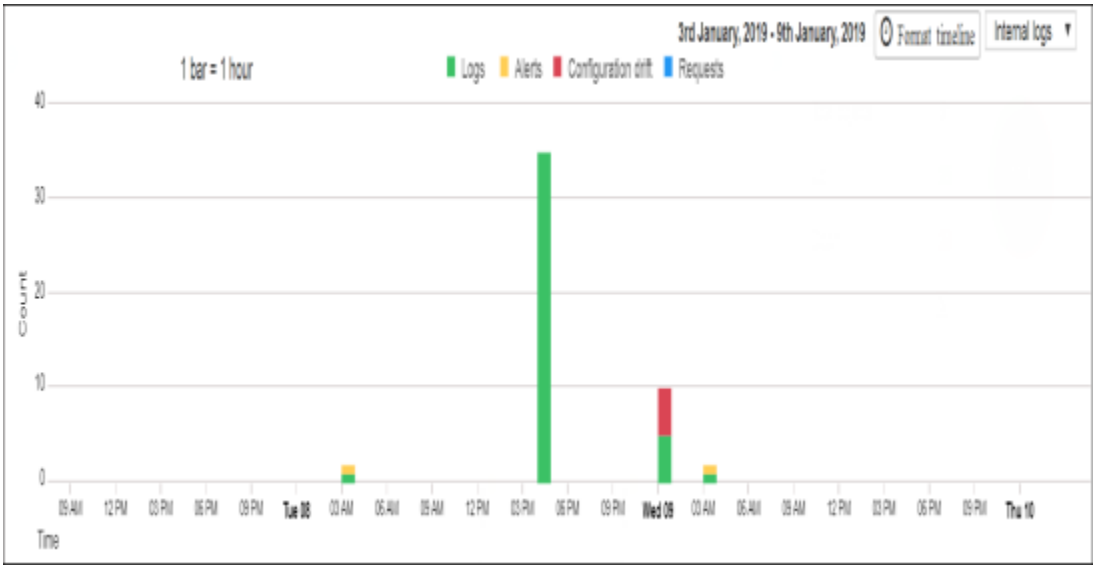
- Object Type
- Vendor

## View AppVision Component Reports

The Reports feature lists all of the reports and alerts related to the specific service components used in the application infrastructure.

To view the reports:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Open the application whose reports you want to view.
3. On the workspace that opens, click Reports.
   A bar chart made up of colored bars displays the total log, alert, configuration drift count, and requests corresponding to the timestamp.




4. Click on the legends (such as Logs, Alerts, Configuration drift, and Requests) to select/deselect the data that you want to be displayed/hid respectively on the chart.
5. Click on the particular bar in the chart to view the corresponding details.

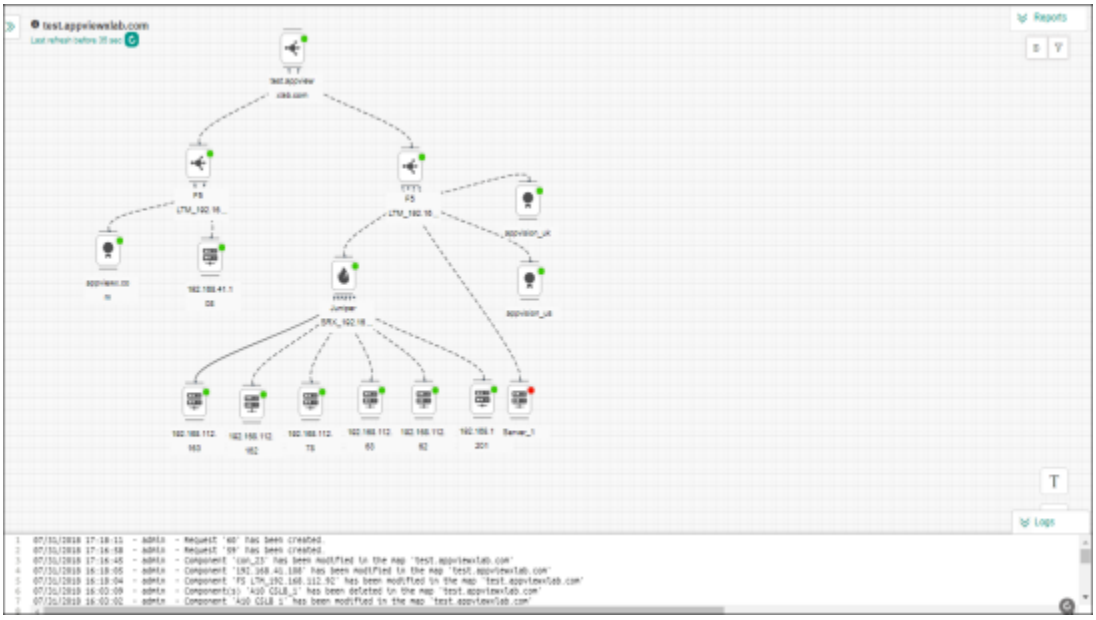
**Note:** You cannot view the components reports for a Blueprint until it is deployed in an environment.

6. Click on the **Format timeline** button to define the time for which you want to view the report.
7. Click on the **Internal logs** dropdown and select the **External logs** option to view the logs generated from Splunk and ELK Stack.

## View Action Logs

To view the logs that list all user-specific actions performed in the AppVision module, complete the following steps:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to see the logs for a Blueprint, click the Blueprint tab to open the application whose logs you want to view.
3. On the workspace that opens, click Logs.
   The logs field appears at the bottom of the screen, as shown below.




## Update an Application Infrastructure

If AppVision fails, the application infrastructures are not managed and monitored by the platform. When AppVision is up and running again, you can select this option to fetch and update the application details from the Tag engine.

To update the application infrastructure:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click in the Command bar.
3. On the **App store** screen that opens, enter the name of the application you want to search by in the search field.
4. Click beside each application name you want to update.
5. Click the **Get** button to fetch and update the selected application details.

## Blueprint

A topological view of an undeployed application infrastructure with all network components like ADCs, firewalls, and certificates logically linked is displayed as a Blueprint.

**Note:** A model Blueprint has been pre-configured to understand the out of box value gained through the Workflow and AppVision platforms. For more details on how to access the model Blueprint, refer to the Out of Box Supportsection of this guide.

## Out of Box Support

To access the model Blueprint:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the **Blueprint** tab.
   A model Blueprint is displayed in the Blueprint inventory.
3. Click on the **Blueprint**.
   The service components such as Wide IP, Virtual Server, Firewalls, and Certificates are used to design this model Blueprint. Deployment of this Blueprint is supported via workflows. For more details on how to deploy a Blueprint, refer to the Deploy a Blueprint section of this guide.

## Create a Blueprint

To create a blueprint:

1. Click and select **AppVision** > **Application**.
   The Application screen opens with the **Inframap** tab selected by default.

2. Click the **Blueprint** tab.
3. Click  in the Command bar.
4. On the Create application blueprint screen that pops up, enter a name for the blueprint.
5. (Optional) In the **Description** field, enter any additional information required for the application.
6. Click the **Save** button.

   A pop-up message is displayed at the top of the workspace: **Blueprint created successfully**.
7. On the navigation bar that appears at the left corner of the workspace, select one of the following tabs.
   -  (**ADC**)
   -  (**Default**)
   -  (**Certificate**)
   -  (**Firewall**)
8. Upon expanding, you can drag and drop the required service components to the workspace. Also, click  or  and enter the name of the component you are looking for.
9. Draw a Link to connect the service components in the workspace.
10. On the **Link selection** screen that opens, enter a name for the Link and then, select the **Link Type** to help the architect by providing the information about routing the component.
11. Click the **Save** button.

    The application infrastructure you designed is saved as a blueprint in the **Blueprint** screen.

## Workspace of a Blueprint

A workspace of a Blueprint is where you design a new application infrastructure. The workspace view allows you to view and perform the following tasks, some of which were discussed earlier under the **Inframap** section of this guide.

- Navigation bar
- Access the Actions Menu
- View the Component Details
- Delete a Service Component
- Provision
- History
- Clone as Blueprint
- View Action Logs

## Provision a Blueprint

Provisioning a blueprint in AppVision enables the user to deploy the application infrastructure by submitting the service request globally across all the components.

To deploy a Blueprint, ensure that the following pre-requisites are met:

- The blueprints should have components and templates (automation tasks) associated with them.
- Templates and workflows should be enabled in the APS/Orchestrator engine.
- You should have the required access permissions to view and submit the service requests for deployment.

You can deploy a Blueprint by one of the following methods:

- Deploy as Request
- Deploy as Code

## Deploy as Request

To deploy a Blueprint using service requests:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the **Blueprint** tab.
3. Open the application infrastructure you have created.
4. On the workspace that opens, all the service components of an application are displayed.
5. You must create a clone of the Blueprint before deploying it. For more details, refer to the Clone as a Blueprint section of this guide.
6. Click the **Provision** dropdown menu and select 

in the Command bar.
   The deployment screen opens with the **Deploy as request** tab selected by default. A list of components used for designing the application is displayed under the **Components** section.
7. Click  beside each service component. The field expands to display a list of actions that are associated with the service component.
8. Drag and drop the templates or workflows to the Service requests section.
9. Click  to arrange the requests in the sequence that you want the automation tasks to be performed.
   Also, you can delete the requests from the request cart by clicking  .
10. Click the **Deploy** button.

The service requests are then deployed in the sequence you designated in the Request cart. A popup message is displayed at the top of the workspace: **Application deployment request submitted**. An Inframap is created when the deployment request starts to retrieve the objects. The pre-validation and post validation scripts help the user ensure that the deployment was successful.

## Deploy as Code

To deploy a Blueprint as a code:

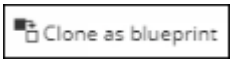
1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the **Blueprint** tab.
3. Open the application infrastructure you have created.
4. On the workspace that opens, Click the **Provision** dropdown menu and select 

in the Command bar.
   The deployment screen opens with **Deploy as Request** tab selected by default.
5. Click the **Deploy as Code** tab.
6. Copy and paste the code file of the application infrastructure that you have saved on your computer.
7. Click **Save Changes** to save the file, which can be deployed later, or click **Deploy** to deploy the Blueprint immediately.

## Clone as a Blueprint

The Clone as Blueprint option allows you to create an exact copy of the application infrastructure with a different name before deploying a Blueprint or to create a backup before making any changes on a live Inframap. You can clone an Inframap or Blueprint only if you have the necessary permissions.

To create a clone:

1. Click and select **AppVision** > **Application**.
   The Application screen opens with the **Inframap** tab selected by default.
2. If you want to create a replica of the application that appears in a Blueprint screen, click the Blueprint tab and do the following.
3. Open the application for which you want to create a backup.
   The workspace of the respective application opens.
4. Click the **More** dropdown menu and select 

in the Command bar.

5. On the **Clone as blueprint** screen that pops up, enter a name for the Blueprint to help the users identify it.
6. (Optional) In the **Description** field, enter any additional information required for the application.
7. Click the **Save** button.
   A popup message is displayed at the top of the workspace: **Application cloned successfully**.

## View the Component Details in Blueprint

To view the details of any component that appears in the Blueprint:

1. Click and select **Appvision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the Blueprint tab and open the application whose details you want to view.
3. On the workspace that opens, right-click the component and select **Details**.
   The Details screen opens with the **Objects** tab selected by default.

> **Note:** You can view the objects associated with the component only after it is deployed in an environment.

4. Click the **Requests** tab to view the list of service requests that have been triggered, along with their status.
5. Click the **Request ID** to view the corresponding request details.
   The request screen opens, showing the work order tasks or phases of the corresponding request in a tree-view. For more details, refer to the Request tasks section of this guide.

## Import an Inframap as Code

AppVision has an option to import an Inframap as code and used them rapidly and easily to deploy in another IT environment.

To import the code for an Inframap:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. Click the **Blueprint** tab and select in the Command bar.
3. On the **Import** screen that opens, enter a name for the Blueprint to help the users identify it.
4. Click the **Browse** button.

5. On the screen that appears, navigate to the file you want to import, click it, and then click **Open**
6. Enable the **Preview** button to view the way the infrastructure looks to end-users.
7. When the Import screen opens again, click **Submit**.

## Edit an Inframap or Blueprint Description

To edit the description of an Inframap or Blueprint:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to edit a Blueprint, click the **Blueprint** tab.
3. Click on the Inframap or Blueprint that you want to modify.
4. On the **Edit Description** screen that opens, modify the description that appears on the **Description** field.
5. Click **Save** to save your changes.

## Upload a File to an Inframap or Blueprint

To upload a file containing additional information to an Inframap or Blueprint, complete the following steps:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to upload to a Blueprint, click the **Blueprint** tab.
3. Click on the Inframap or Blueprint to which you want to upload a file.
4. On the **Upload** screen that opens, click **Browse** and navigate to the file you want to add, then click **Open**.
5. When the Upload screen opens again, click **Upload**.

## Download a File from an Inframap or Blueprint

To download a file that is associated with an Inframap or Blueprint, complete the following steps:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to download from a Blueprint, click the **Blueprint** tab.

3. Click  on the Inframap or Blueprint whose file you want to download.
4. On the **Download** screen that opens, select the file and click  . The file is downloaded to your computer.
5. Navigate to the location where you want the file to go, then click **Save**.

## Delete an Inframap or Blueprint

To remove Inframapsor Blueprintsthat need not be managed in AppVision:

1. Click  and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to delete a Blueprint, select the application infrastructure from the **Blueprint** tab and click  on the card view of the applications.
   If the applications are already selected,  appears.
3. Click  in the Command bar.
4. You can also click  on the card view of the respective applications to delete them.
5. On the **Confirmation** screen that pops up, click **Yes**.

# Service



## Add a Service Component

To add a service component:

1. Click  and select **AppVision** > **Service**.
   The Service screen opens.
2. Click  in the Command bar.
   The **Create Component** screen appears.
3. In the **Basic-Info** section, enter a name for the new component.

4. In the Type dropdown list, select the type of component you want to create:
   - **General** - These are the service components that are displayed on the Inframap workspace.
   - **Link** - These are the dotted lines that transfer information from one component to the other.
   - (Optional) In the Description field, enter any additional information required for the component.
   - In the Group name dropdown list, select how you want to group the components you created: ADC, CERT, Firewall, and Default.
   - Click Upload an image and then navigate to the image that you want to use to logically represent the component in the workspace.

   **Note:** You can assign any number of actions to a component. To view the template or workflow associated with a particular action, hover your cursor over the Action name inside the **Action Name** field.

5. In the Action Name field, enter the name of an automation task you want to make available in the component's action menu. Select a template or workflow from the dropdown list based on the automation task you want to associate with the component.
6. Click **Add**.
   The action then appears inside the **Action name** field.
7. Repeat the above steps for each additional action you want to make available through the component.
8. Click **Submit** to add the component.
   The customized component you just created is then added to the **Service** inventory.

## Update a Service Component

To update a service component:

1. Click and select **AppVision** > **Service**.
   The Service screen opens.
2. On the **Service** screen, click the component you want to modify in the Service pane.
3. On the **Update Component** screen that appears, make changes to any or all of the following fields:
   - Description
   - Group name
   - Upload an image
   - Action name
   - Template or Workflow
   - Click **Add**.

- The action name and the template associated with a component populates inside the **Action name** field.
- Click **Submit** to update the component.

## Delete a Service Component

To delete a component:

1. Click and select **AppVision** > **Service**.
   The Service screen opens.
2. From the Service inventory, click on the component you want to delete.
3. Click in the Command bar.
4. On the **Confirmation** screen that pops up, click **Yes**.

## Service Pane

The Service pane allows you to configure and publish service components such as ADC, Certificates, Firewalls, and other user-defined components that are used for modeling application infrastructures on-premises or on the cloud. With the Service pane, you can create new components or edit existing vendor-specific components and can associate them with a range of customizable templates or workflows to handle the automation of infrastructure tasks. You can also delete, refresh, search, and update service components through the Service screen.

# Chapter 5: Studio

## Studio Module

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

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

## Workflow Tasks

The Workflow screen within the Studio module allows you to perform the following tasks:

- Switch Between List View and Card View
- Configure the Settings for a Workflow
- Create a Workflow
- Enable a Workflow
- Run a Workflow
- Disable a Workflow
- Modify a Workflow
- Validate a Workflow
- Clone a Workflow
- Import a Workflow
- Export a Workflow
- Delete a Workflow
- Bookmark a Task
- Import a Task
- Create a Subflow
- Import a Subflow
- Create a Rollback Workflow
- Import a Rollback Workflow
- Create a Folder
- Auto Align Tasks
- Clone a Subflow
- Rename a Subflow
- Delete a Subflow

## Switch Between List View and Card View

The contents of the Workflow Configurator screen can be viewed as a list or as a series of cards. The view you want to access will depend on the kind of task you are trying to complete. The card view allows you to perform tasks directly from each card, while the list view is better suited to performing global actions and comparing the workflows to each other.

To switch between the two views:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears by default.
2. To switch to the list view, click in the Command bar.
3. To switch back to the card view, click in the Command bar.

## Configure Workflow Settings

To configure the settings of a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen opens with a list of workflows.
2. Click the workflow whose settings you want to configure. The workspace corresponding to the workflow opens.
3. Click at the top of the screen.
   The **Settings** screen appears.
4. Configure any of the settings on the following tabs:
   - General
   - Assign workflow
   - Workflow
5. Click **Save**.

## Create a Workflow

To create a workflow in AppViewX:

**Note:** You can double-click the **Stop** action to define a rule to trigger an auto rollback or an associated cleanup workflow.

**Note:** To rename a task that is created and configured, you can double-click it and then click .

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Click in the Command bar.
3. On the New workflow screen that appears, enter a name for the new workflow.
4. (Optional) Provide additional details about the workflow.
5. (Optional) From the **Category** dropdown, select the group to which the workflow must belong.
6. Click the Create button to add the workflow to the system.
   The new workflow workspace appears.
7. Upon clicking, the following sections and corresponding tasks appear on the left side of the workspace:
   - **Search**
   - General
     - **Delay** - Configure custom delay intervals between workflow tasks.
     - **If** - Configure different actions to be performed upon the success or failure of a task in a workflow.
     - **Switch** - Group a set of rules to trigger multiple sets of actions in a workflow.
     - **Retry** - Configure the specific time or interval at which the execution of a work order must be retried.
     - **Work order** - Add child work orders to a parent work order. The child work order consists of one or more tasks.
     - **Join** - Connect two or more parallel flows in a workflow.
     - **REST** - Define URLs of the external APIs (along with the authorization and required headers) to be triggered.
     - **REST(I)** - Define the internal APIs to be triggered.
     - **Split** - Trigger parallel set of tasks at the same time.
     - **Schedule** - Plan one or more tasks in a workflow to be executed at a particular period.
     - **Dependency** - Decide the execution of tasks based on the completion of particular tasks.
     - **Script** - Use Python scripts to be executed in a workflow. You can create one or more Python scripts, which can be dragged and dropped to the workspace later on.
     - **Loop** - Define a sequence of instructions to be repeated continually until a certain condition is reached.
     - **BreakLoop** - Define a condition upon reaching which a loop must be terminated.
     - **Implementation**
     - **Prevalidation**
     - **Post validation**

- **Rollback**
- **Ansible Executor** - Configure an Ansible host instance and path to discover the playbooks.

- User interface
  - **Form** - Use a form builder along with the custom associate script. This task consists of four tabs, namely, **Information**, **Form Builder**, **Hooks**, and **Roles & settings**. You can define the Global variables in the **Roles & Settings** tab or click the field in the **Form Builder** tab.
  - **Grid** - Display the provided data in the form of an editable or non-editable table.
  - **Review** - Display the final editable or non-editable commands in the script that have been implemented in the device.
  - **Chart** - Display the provided data as a pie, bar, or stacked bar chart.
  - **YAML** - Provide input in YAML format, which is very easy to understand. You can also import playbooks into Studio.
  - **Diff Checker** - View side-by-side comparisons of configuration files.
- ITSM - Click **Change** and the following tasks appear:
  - **Create** - Create a ticket in ServiceNow.
  - **Close** - Close a ticket in ServiceNow. The details of a closed ticket cannot be edited.
  - **Get** - Retrieve the details of a ticket from ServiceNow.
  - **Push Config** - Push the data into a particular ticket in ServiceNow.
  - **Push Logs** - Push the logs into a particular ticket in ServiceNow.
  - **Validate** - Validate the ticket created in ServiceNow using the Create option.
  - **Withdraw** - Remove a ticket from ServiceNow. The details of a withdrawn ticket can be edited.
- **Notification**

**Note:** If the SMTP is not configured in the AppViewX settings, an email notification will not be sent and the event will be recorded in the Audit logs.

  - **Email** - Configure an auto-generated email that is triggered along with the workflow data. These emails can be configured with various levels of approval required to trigger a workflow. You can create one or more email templates that can be dragged and dropped to the workspace later on. Also, you can do the following:
    - Attach the global variables available in the workflow.
    - Browse and attach other files from your PC.
  - **Slack** - Send notifications through Slack as a part of the workflow process.
  - **PagerDuty** - The PageDuty users will receive a notification on their device. This is based on the information they have provided their PagerDuty account.
- **Folders**

- **Add** - Create a new user or global folder in which you can place your tasks, workflows, or sub-workflows.
- **Import** - Import tasks from other workflows to a specific folder of your choice.
- **Default** - The contents of this folder will be deleted once you exit the workflow.

- **Integrations** - View the external entities that are integrated with the Studio module.
- **FAQ** - Use the ready-made tasks that are most commonly used to design a workflow.
- **Store** - View the multi-level folder hierarchy for the Out of the Box (OOB) tasks and flows.

8. Drag and drop the tasks you want to the workspace and fill in a minimum of all the mandatory fields for each task in the following sections:
   - **General** - Consists of all the details and the configurations of the task.
   - **Global variables** - Consists of pre-defined values that can be reused in other tasks. In a workflow, you can click  in the command bar to view all the variables that have been defined.
   - **Custom message** - Consists of text messages that must appear during various stages of the task.
   - **Action** - Consists of labels that can be defined for the tasks depending on their statuses. These labels will be displayed in the tree-view of the workflow upon the success or failover of a task.
9. Create a workflow using connectors between the tasks as appropriate. You can click  in the command bar to select one of the following types of connectors you want to use in the workflow:
   - **Default**
   - **Flow**
   - **Curved**
   - **Straight**

> **Note:** When you use a second outgoing connector from a task, a **Link Selection** window appears, in which you can define the **Flow Type** and provide a **Display Name** for it.

## Enable a Workflow

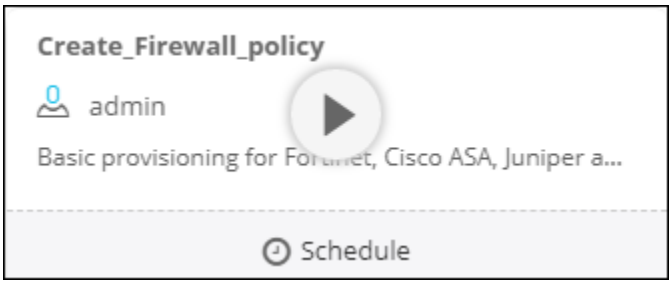
To enable workflow in AppViewX:

1. Click  and select **Studio** > **Workflow**.
   The Workflow screen opens.
2. Click the workflow you want to enable.
3. On the **Card view**, you can click  on the respective workflows to enable them.
4. Click  in the Command bar.
5. On the Confirmation screen that appears, click **Yes**.

# Run a Workflow

To run a workflow in AppViewX:

1. Click and select **Workflow** > **Request**.
   My Workflows screen opens.
2. Click the **Play** button on the workflow, which you want to execute.




3. On the screen that opens, the **Request View** tab is selected by default.
4. At a minimum, fill in all fields that contain a red asterisk beside their names.
5. Click the **Submit** button.
   A new request ID is created to view the request details. The **Request View** tab displays the tasks or phases of a request in a tree view after the workflow execution is complete.

> **Note:** After you submit the request form, the configuration changes are reviewed and implemented only after approval.

6. Click on each task to view its details.
   All logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.
7. Click the **Workorder View** tab to view the work order details such as work order ID, date, and time when the work order was created and updated, status, RFC ID, and RFC status.

# Disable a Workflow

To disable a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Configurator screen opens.
2. Click the workflow you want to disable.

**Note:** On the **Card view**, you can click on the respective workflows to disable them.

3. Click in the Command bar.
4. On the Confirmation screen that appears, click **Yes**.

## Modify a Workflow

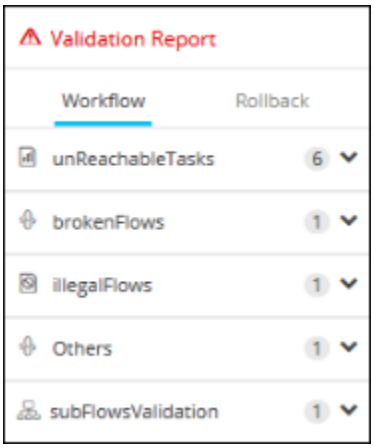
To edit a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen opens.
2. Click the workflow you want to edit.
   The **Modify** screen appears.
3. Make whatever changes are required.
4. Click to ensure the changes you made did not break the workflow.

## Validate a Workflow

To validate a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen opens listing all the workflows in the system.
2. Click the workflow you want to validate.
   The workspace corresponding to the workflow opens.
3. Click at the top of the screen.
   If the workflow is valid, a validation message appears at the top of the screen. If the workflow is invalid, the details are displayed in the Validation Report pane in the workspace, a sample of which is shown below.




4. You can click ☑ or ☒ beside each section to view or hide the details respectively.

## Clone a Workflow

To clone workflow in AppViewX:

1. Click ☰ and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Select a workflow for which you want to create a replica.
3. Click ❐ in the workflow Command bar.
4. On the **Clone Workflow** screen that appears, enter a name for the new workflow.
5. (Optional) Enter a description that helps differentiate this new workflow from the original.
6. Click **Save** to add the workflow to the system.
   The cloned workflow workspace appears with all the data that was in the parent workflow. Also, the cloned workflow will be executed immediately after the cloning is complete.

## Import a Workflow

To import one or more workflows into AppViewX:

1. Click ☰ and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Click the **Import** option on the left.
3. On the Import screen that appears, click **Browse**.
4. Select the zip file containing one or more workflows, then click **Upload**.
5. Click **Submit**.

## Export a Workflow

To export a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen opens.
2. The Workflow screen opens.
3. Click the workflow you want to export.

> **Note:** On the **Card view**, you can click on the respective workflows to export them.

4. Click in the Command bar.
5. On the Export confirmation screen that appears, click **Yes**.
   The workflows are exported to your computer as a zip file.

## Delete a Workflow

To modify a workflow in AppViewX:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen opens.
2. Select one or more workflows to delete.
3. Click in the Command bar.
4. On the **Delete** confirmation screen that appears, click **Yes**.

## Bookmark a Task

To bookmark a task in Studio:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Click the required section on the left side.
   The tasks corresponding to the section appear.
3. Drag and drop the task of your choice to the workspace.
4. In the task creation screen that appears, click .

The **Save to Folder** screen appears.

5. Select the folder in which the task must reside and click **OK**.

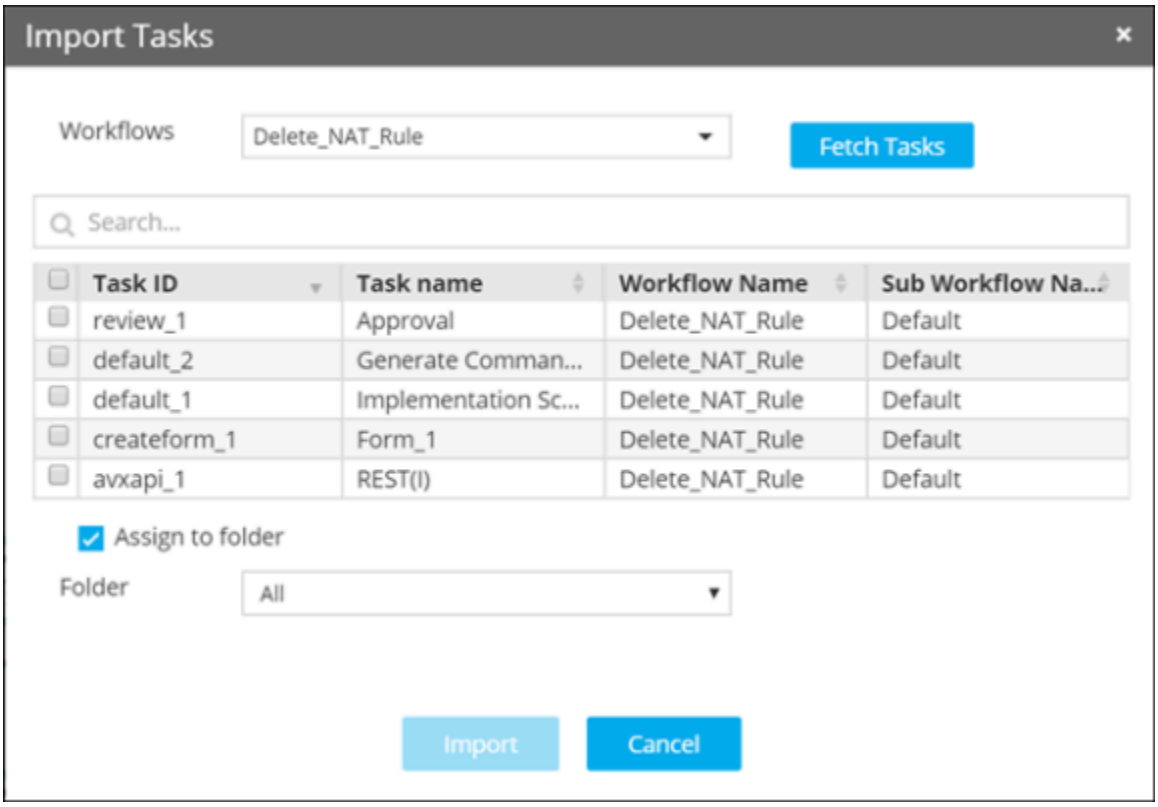
## Import a Task

To import a task a specific folder of your choice:

1. Click  and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Click the Folders section on the left-hand side.
3. Click **Import**.
   The **Import** Tasks screen appears.

> **Note:** If you do not use these options, the tasks will automatically be imported to the **Default** folder. All the tasks added to this folder will be deleted once you exit the workflow.

4. From the **Workflows** dropdown list, select the required workflow.
5. Click **Fetch Tasks**. A list of all the tasks corresponding to the selected workflow is displayed.
6. Select the required task(s).
7. Select the **Assign to folder** check-box if you want to import the task(s) to a specific folder of your choice.
8. From the **Folder** dropdown, select the folder to which the task(s) must be imported.




9. Click **Import**. The selected tasks are added to the selected folders.
10. Click the required folder to display all the tasks it consists of. You can drag and drop those tasks to the workspace whenever required.

## Create a Subflow

You can organize huge workflows better with the help of nested/subflows.

**Note:** These subflows will be a part of the workflow in which they have been created and hence, will not appear in the workflow inventory page.

**Note:** Subflows appear in green within the workspace.

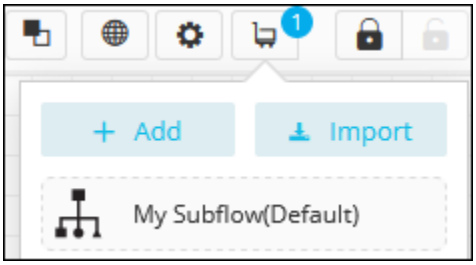
To create a subflow within a workflow:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears.

2. Create a new workflow or select an existing workflow to which you want to add a subflow.
3. Click and click **Add** on the screen that appears. The **New Subflow** screen appears.
4. In the **Name** box, provide a name for the subflow.
5. (Optional) In the **Description** box, provide additional information related to the subflow.
6. Click **Create** to add the subflow to the **Workflows** tab. The subflow workspace appears.

   For more information on the sections and tasks that appear on the left-hand side, refer to steps 6 and 7 in Create a workflow section of this guide.
7. Go back to the parent workflow and click .

   The new subflow appears along with its category name in the **Workflows** tab.




8. Drag and drop the subflow to the workspace and link it with the parent workflow as required.

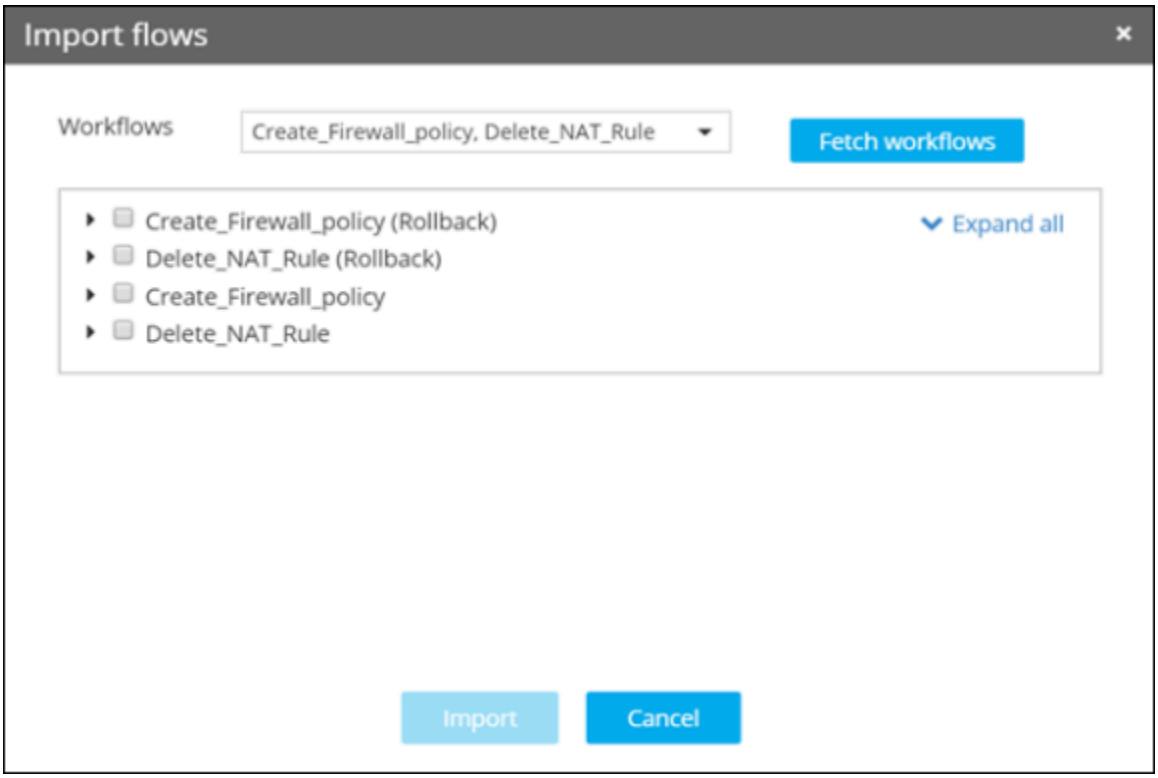
## Import a Subflow

To import the existing workflows as subflows into other workflows:

1. Click and select **Studio** > **Workflow**.

   The Workflow screen appears.
2. Create a new workflow or select an existing workflow to which you want to add a subflow.
3. Click and click **Import** on the screen that appears.

   The **Import Flows** screen appears.
4. From the **Workflows** dropdown list, select the required workflow.
5. Click **Fetch Workflows**. A list of all the workflows is displayed.
6. Select the workflows that must be imported as subflows.




7. Click **Import** to add the selected workflows to the **Workflows** tab.
8. Drag and drop the subflow to the workspace and link it with the parent workflow as required.

## Create a Rollback Workflow

You can define a rollback workflow that must be triggered when a workflow fails while execution.

**Note:** A rollback can be performed only on the completed workflows.

**Note:** Rollback workflows appear in green within the workspace.

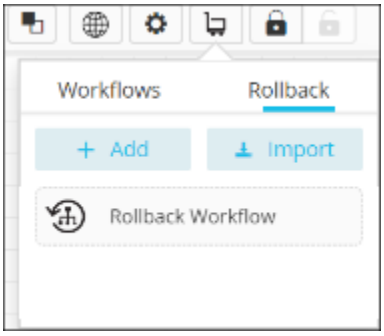
To add a rollback workflow:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. On the **Workflow** screen, create a new workflow or select an existing workflow to which you want to add a subflow.
3. Click the **Rollback** tab on the screen that appears.

4. Click and click **Add** on the screen that appears.
   The **New Subflow** screen appears.
5. In the **Name** box, provide a name for the rollback workflow.
6. (Optional) In the **Description** box, provide additional information related to the rollback workflow.
7. Click **Create** to add the rollback workflow to the **Rollback** tab.
   The rollback workflow workspace appears.

> **Note:** For more information on the sections and tasks that appear on the left-hand side, refer to steps 6 and 7 in the Create a workflowsection of this guide.

8. Go back to the main workflow and click the button.
   The new rollback workflow appears in the **Rollback** tab.




9. Drag and drop the rollback workflow to the workspace and link it with the main workflow as required.

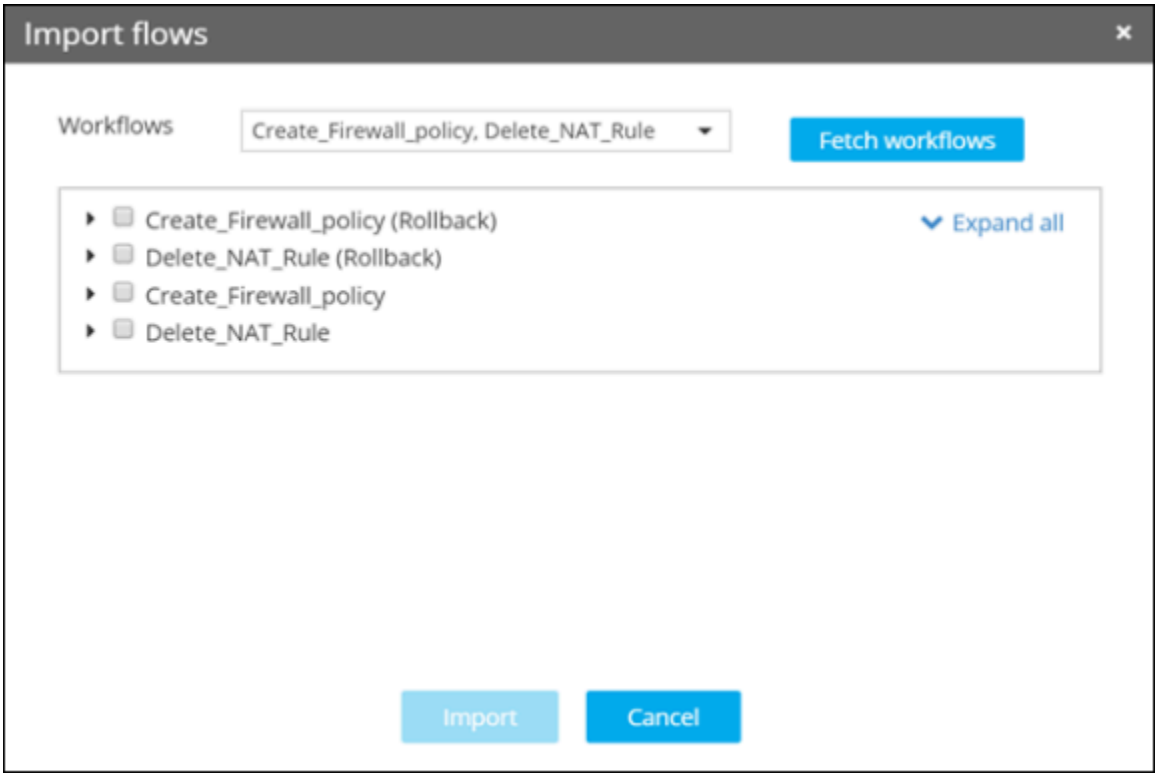
## Import a Rollback Workflow

You can import an existing workflow that must be triggered when a workflow fails while execution.

To import a workflow as a rollback workflow:

1. Click and select **Studio** > **Workflow**.
   The Workflow screen appears.
2. Create a new workflow or select an existing workflow to which you want to add a subflow.
3. Click the **Rollback** tab on the screen that appears.
4. Click and click **Import** on the screen that appears.
   The Import flows screen appears.
5. From the **Workflows** dropdown list, select the required workflow.
6. Click **Fetch workflows**.A list of all the workflows is displayed.

7. Select the workflows that must be imported as rollback workflows.



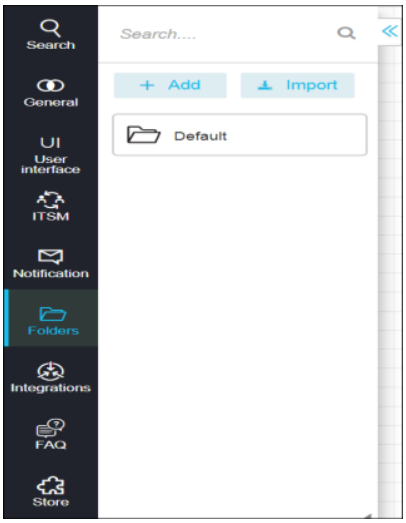

8. Click **Import** to add the selected workflows to the **Rollback** tab.
9. Drag and drop the rollback workflow to the workspace and link it with the main workflow as required.

## Create a Folder

You can group tasks according to various categories using folders.

To create a folder in a workflow:

1. Click and select **Studio** > **Workflow**.
2. On the **Workflow** screen, create a new workflow or select an existing workflow to which you want to add a folder.
   Each workflow will have a **Default** folder. All the tasks added to this folder will be deleted once you exit the workflow.
3. Click **Folders**.



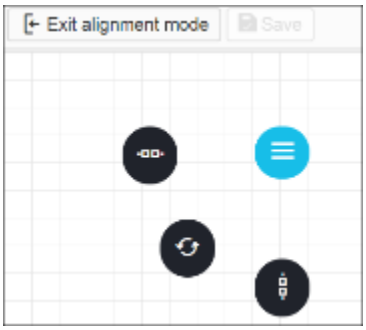

**Note:** For more information on the sections and tasks that appear on the left-hand side, refer to steps 6 and 7 in the Create a workflow section of this guide.

4. Click **Add**. The **Create Folder** screen appears.
5. In the Folder name box, enter a name for the folder you want to create.
6. Enable the option **Global** if you want the folder to be accessible by all the users. If you want the folder to be accessible only by you, leave the option **Global** disabled.
7. Click **Add**.
   The new folder that you created is displayed on the left-hand side of the screen.

## Auto-Align Tasks

To auto-align tasks in a workflow:

1. Click and select **Studio** > **Workflow**.
2. On the Workflow screen, click the workflow you want to auto-align.
3. Click the **Auto-align** button.
4. In the confirmation dialog box that appears, click **Yes**.
   The workflow enters into the auto-alignment mode.




5. You can click one of the following:
   -  to place all the tasks horizontally.
   -  to place all the tasks vertically.
   -  to align the tasks to their original position.
6. Click **Save** to retain the alignment you have chosen.
7. Click **Exit alignment mode** once you are done auto aligning your workflow.

## Rename a Subflow

To rename a subflow in AppViewX:

1. Click  and select **Studio** > **Workflow**.
   The **Workflow** screen opens, listing all the workflows in the system.
2. Click the workflow whose subflow you want to rename. The workspace corresponding to the workflow opens.
3. Right-click the subflow you want to rename.
4. From the pop-up menu that appears, click **Rename**.
5. Type a new name for the subflow.

## Clone a Subflow

To clone a subflow in AppViewX:

1. Click  and select **Studio** > **Workflow**.
   The **Workflow** screen opens, listing all the workflows in the system.
2. Click the workflow whose subflow you want to clone.

The workspace corresponding to the workflow opens.

3. Right-click the subflow to create a replica.
4. From the pop-up menu that appears, click **Clone**.
   The cloned subflow appears in the workspace.

## Delete a Subflow

To delete a subflow in AppViewX:

1. Click  and select **Studio** > **Workflow**.
   The **Workflow** screen opens, listing all the workflows in the system.
2. Click the workflow whose subflow you want to delete. The workspace corresponding to the workflow opens.
3. Right-click the subflow you want to delete.
4. From the pop-up menu that appears, click **Delete**.
5. From the **Confirmation** dialog box that appears, click **Yes**.

## Reports Tasks

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

- Create a report
- Clone a report
- Delete a report

## Create a Report

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

1. Click  and select **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. Click **Create New Report**.
3. In the **BASIC INFO** screen of the report creation wizard:
   a. Enter a **Name** for your report.
   b. (Optional) In the **Description** field, type additional information related to the report.

c. Click **Yes** if you want to control the access to the report using different permissions for different users.
d. Click **Save** resume the chart creation later or click **Next** to proceed with the chart creation.

4. In the **DATA SOURCE** screen:

a. 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).

b. Click **Save** resume the chart creation later or click **Next** to proceed with the chart creation.

5. In the **CHART CONFIGURATION** screen:
   a. Click on one of the following reports to **Select chart type** - **PIE**, **DONUT**, **BAR**, **STACKED BAR**, **GRID**, **LINE**, and **METRIC**.
   b. The fields that appear vary for each chart type, at a minimum, fill in all the mandatory fields.
   c. Click **Save** resume the chart creation later or click **Next** to proceed with the chart creation.
6. In the **CHART DRILLDOWN** screen:

a. Select the checkbox to view more specific layers of the data or information being analyzed.

b. 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.

7. Click **Save & Enable** to save the report to the AppViewX system.
   The report is added to the **My reports** tab, it can be enabled or disabled using the toggle button in the **Status** column.
8. 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.

## Clone a Report

To clone a report:

1. Click  and select **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 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**.

## Delete a Report

To delete one or more reports:

1. Click  and select **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**.

## Rules Tasks

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

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

## Create a Rule

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

1. Click  and select **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. From the dropdown, select a workflow that must be triggered when the rule criteria are met.

> **Note:** An OOB workflow with ServiceNow integration for tracking and Email capability will be shipped. Those workflows will be available under the category rules in Studio. You can either customize the workflow further or associate it with any of the above actions. If the rule is active, the actions executed from AppViewX will trigger the associated workflow.

> **Note:** You can define rules only for the ADC object actions (Enable, Disable, Graceful Disable, Forcedown, Enable all, Disable all, Forcedown all, Enable Persistence, Disable Persistence, Forcedown Clear Active, Clear Ram Cache, Clear Persistence, Object restore/Rollback, Device restore/Rollback, and Class management changes/Rollback).

7. (Optional) Define the **Rule criteria**.

> **Note:** Only the action payload can be configured in the criteria. Only one rule can remain active for action at a time.

## Clone a Rule

To clone a rule:

1. Click and select **Studio** > **Rules**.
   The Rules screen displays a list of all the rules.
2. Select the rule you want to clone.
3. From the **Actions** dropdown, click **Clone**.
4. In the screen that appears, enter a **Name** for the cloned rule.
5. 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.

## Delete a Rule

To delete one or more rule(s):

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

## Request Tasks

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

The **Request** section of the Studio module consists of the following tabs:

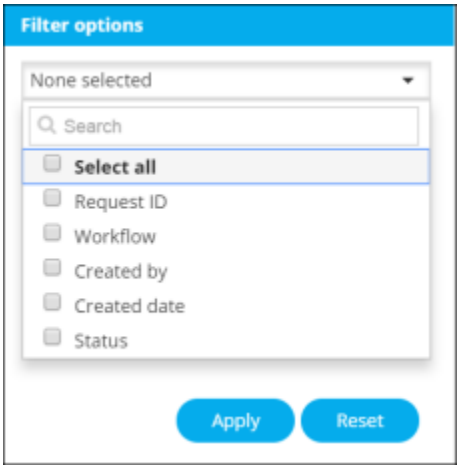
- **Overview** - Consists of the following three sections:
  - **Dashboard** - Displays the total number of all, open, closed, and failed requests.
  - **Total requests** - A pie chart containing the percentage of requests in four different statuses, namely, **In progress**, **Completed**, **Failed**, and **Rollback**.
  - **Total requests by a workflow** - A bar chart displaying the number of requests from the workflows selected through .
  - **Change submission request** - A line chart displaying the total number of change submission requests segregated based on daily, weekly, monthly, quarterly, and yearly.
- My workflows - Consists of the following two sections:

- **View/Run** - Displays all enabled workflows assigned to a specific user role. On this screen, you can perform the following tasks:
  - Search for a workflow using the **Search** field. You can click  to search for a workflow in the categories of your choice. Also, you can arrange the workflows in **Ascending**, **Descending**, or **Recently** created order using the **Sort by** option beside the search field.
  - Click  to define the time, duration, and frequency of a workflow.
  - Click  to trigger a workflow immediately.
- **Scheduled jobs** - Displays all workflows that have been scheduled. A unique Job ID is created every time a scheduled workflow is triggered. From the Job ID column, you can click on the job for which you want to view the details.

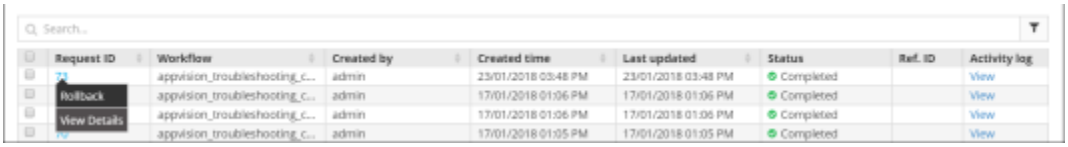
- My requests - Displays the total number of **All**, **Open**, **Closed**, and **Failed** requests, clicking upon these tabs displays the corresponding workflow details in a table.
- From the **Request ID** column, you can click on the request for which you want to view the details. On the tabs in this screen, you can perform the following tasks:

**Note:** For the workflow(s) containing grid component(s) and script(s) to generate data, you can click  to save the data to PC in XLS or CSV file format.

- Search for a request using the **Search** field and clicking  to select the options you want to use to sort the requests.



- Click the **Request ID** to display the tasks or phases of a request in a tree-view. You can click a task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.
- 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.




- Click **View** in the **Activity log** column to display the request in a stage-view. In the **Summary** tab, click  to view the details of a task. Click the Details tab to view log messages and other particulars of a request.
- **Audit logs** - Displays a list of all the events that took place in the Workflow module. Using the **Search** field, you can search for the logs on a particular workflow.

## OOB Tasks

To create a workflow, you can navigate to **Studio** > **Workflow** and then select  .

To create a flow, the user can create a form to get the respective inputs and then select the tasks from the respective section and add them.

In the Workflow tab, when you place tasks in a particular order (forward flow) the same tasks should be placed in the reversed order (reverse flow) in the Rollback tab to perform the rollback operation.

The tasks are categorized into two based on the type of execution: **Immediate** and **Deferred**.

- When the **'is_deferred_execution'** flag is unset, they are known as Immediate tasks and they are executed within the task itself.
- When the **'is_deferred_execution'** flag is set, they are known as deferred tasks and they generate a command(s) which is later fed into the command consolidator.

The command consolidator consolidates commands from all the tasks. The output of the command consolidation task is fed into the implementation task for execution.

The OOB section within the **Studio** contains the following vendor tasks:

- F5
- Infoblox (DNS)
- Firewall Panorama (Beta)



## Add Tasks from F5

1. Click the **Store** icon from the Menu.
2. Select the **Application Delivery Section** and then choose **F5**.
   You can now drag and drop tasks from the list of available tasks.

> **Note:** The currently supported version for F5 is v11. v12, v13, and v14.

> **Note:** For the tasks there are certain flags which control their behavior:
> - **is_deferred_execution:** This flag can be set to generate the commands or unset to execute the task immediately and carry out the required operation within the workflow.
> - **is_rollback:** In a task, this flag can be set along with 'rollback_input' to carry out the rollback operation. (The 'rollback' output of the previous execution has to be fed to ' rollback_input' )
> - **operation_type:** You can perform create, modify, and delete operations using this flag.
> - **is_skip_required:** This flag can be set to skip the execution of a particular task in the workflow.
> - **is_stop_workflow_on_failure:** This flag can be set to stop the workflow execution in case of any failure.
> - **tabular_input:** This input (list of JSON) can be used to carry out multiple object operations in single task execution. Using the tabular input, the actions can be mixed (create, modify, and delete) and it can be carried out in one attempt. Performing a rollback can also be performed in one attempt.

Pre-validation will be performed before the implementation and post-validation will be carried out after the implementation.

## Adding the Command Consolidator and Implementation Task

To consolidate the commands of all the tasks and also to make the rollback function feasible, the command consolidator task must be included after adding tasks from the OOB store.

To add the command consolidator:

1. Click the **Store** icon from the Menu.
2. Select the **Application Delivery Controller** section and then choose **F5**.
3. Select the **Other Modules** folder. Search for the Command Consolidator.
   You can now drag and drop the Command Consolidator by searching for it in the search bar and select it.
4. Once added, you can double click the command consolidator and then maximize the script window.
5. In the script, you can uncomment and enter the unique task ID of all the tasks connected to the Command Consolidator (This process is also known as IO mapping).
6. Once this is done, you need to add the Command Implementation task to execute the commands. You can add the Command Implementation task by searching for it in the search bar present in the **Store** menu and connect it to the Command Consolidator.


The following are the outputs of the command consolidator which are set as global: rollback, implementation, pre_validation, post_validation, partial_rollback.

- **rollback**: This contains the rollback data of all the IO mapped tasks. In the Rollback flow, the 'rollback_input' should be fed from the rollback.parent_task_id
- **implementation, pre_validation, post_validation, partial_rollback**: These fields should be fed to the implementation palette individually. (Approval and review palettes can be added in between if needed.)

## Add Tasks from Infoblox (DNS)

1. Click the **Store** icon from the Menu.
2. Select the **DDI** section and then choose **Infoblox**.
   You can now drag and drop from the list of available tasks.

## Add Tasks from Firewall Panorama (Beta)

1. Click the **Store** icon from the Menu.
2. Select the **Security** section and then choose **Panorama**.
   You can now drag and drop from the list of available tasks.

# Chapter 6: Provisioning



## Add a Regular Expression (RegEx) to the Library

To add a regex pattern to the RegEx Library:

1. Click  and select **Provisioning** > **Template**.
   The Template screen opens.
2. Click  in the Command bar. The Regex Library opens, displaying each of the regex strings in the AppViewX system.
3. Click **+ Add New Regex** at the top of the screen.
4. In the New regex field to the right, enter a Validation name for the regex.

**Note:** This cannot be changed after it is created, so make sure it is readily understandable and concise.

5. Enter the regex string.
6. (Recommended) Enter a notification that will appear if users enter invalid strings in the corresponding field.
7. Click **Add** to save the new regex pattern to the Regex Library.

## Add a Script to the Helper Script Library

To add a script to the Helper Script Library:

1. Click  and select **Provisioning** > **Template**.
   The Template screen opens.
2. Click  in the Command bar. The Helper script Library screen opens, displaying each of the helper scripts in the AppViewX system.
3. Click  in the Command bar.
4. On the **Add** screen that appears, enter a name for the script.

   **Note:** This cannot be changed after it is created, so make sure it is readily understandable and concise.

5. In this release, only Python scripts can be created in AppViewX, so leave the Type field set to the default Python setting.
6. (Recommended) Enter a brief description of what the script does and how it should be used.
7. Type or copy the Helper Script into the Script field.
8. Click **Save** to add the script to the Helper Script Library.

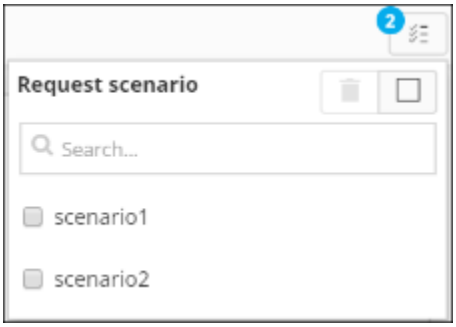
## Create a Request

The details on how to create a request vary depending on which request template you are using. The following instructions provide only a basic overview of the process. Refer to the Create a Template topic for details on the kind of content that should be inserted into specific fields.

To create a request:

1. Click  and select **Provisioning** > **Request**.
   The Request screen opens.
2. Click  on the top-right.

3. On the Create screen that opens, select the name of the template you want to use.
4. Add values in all of the required fields, which are designated by a * beside their names.
5. Click **Add** to append a request scenario to the selected template.




   This links a device and pool to the request. All appended requests are displayed in the top-right corner.
6. Make any other changes you want to the optional fields on the screen.
7. When you have finished, click Save draft to save the new request to the Request list or Submit to make the request.
   If you saved the request as a draft, it appears on the Request screen with a status of Draft. If you submitted the request, it appears with a status of **Open**.

## Roll Back a Work Order

To roll back a work order, it must have a status of **Failed** or **Closed**/**Completed** and it must have a defined workflow.

To roll back a work order:

1. Click and select **Provisioning** > **Request**.
   The Request screen opens.
2. If the request whose work order you want to roll back is not visible on the screen, run a search for the request.
3. Click the link in the **Request ID** column for the request.
4. On the request details screen that opens, click the Work order tab.
5. Select the checkbox beside the Work order ID.
6. Click in the Command bar.
7. On the confirmation screen that pops up, click **OK**.
   The work order is then rolled back and the request returns to its prior state.

# Collection Tasks

Collections serve as generic repositories that hold any data in key-value pair format and act as interfaces for entering and modifying data into the AppViewX Mongo database. Data from collections can be consumed as a part of the provisioning request process or by any other scripts that can be triggered by AppViewX. The structure of the collections is based on the Mongo database.

The Collection screen within the Provisioning module allows you to perform the following tasks:

- Create a collection
- View the details of a collection
- View the activity log for a collection
- Append a collection
- Download a collection
- Export a collection
- Import a collection
- Modify a collection
- Delete a collection

# Create a Collection

To create a collection in AppViewX:

1. Click  and select **Provisioning** > **Collection**.
   The Collection screen opens.
2. Click  in the Command bar.
3. On the Create screen that appears, enter a name for the new collection.
4. Enter the key pair value, using which the collection must be grouped and organized in the **Group by** and **Order by** fields respectively.
5. Enter the unique key pair value to be used for identifying the collection in the **Unique Key** field.
6. (Optional) Enter a date in the field **Date fields**. (Optional) Select the required date format from the **Date format** dropdown list.
7. Map the key pair values in the **Value** field in a valid JSON format.
8. Click **Save** to add the collection to the system.

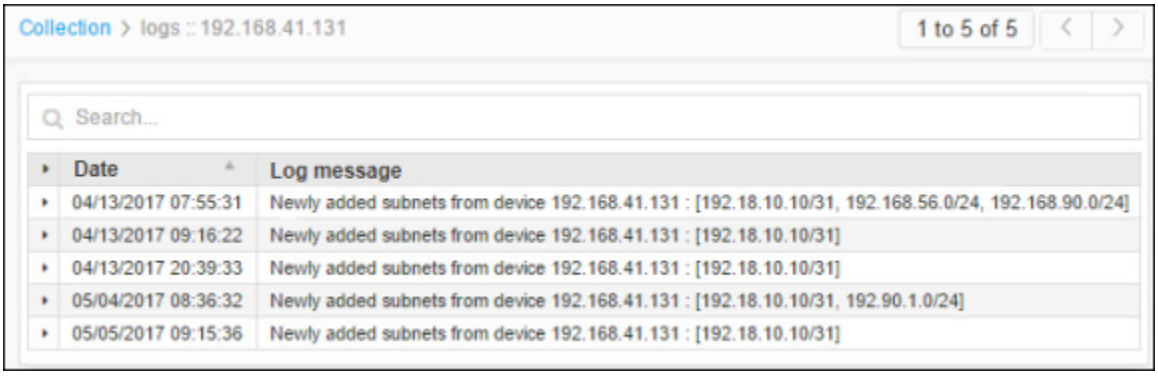
# View the Details of a Collection

To view the details of a collection in the AppViewX system,

1. Click and select **Provisioning** > **Collection**.
   The Collection screen opens, displaying all provisioning collections in the system.
2. If the collection whose details you want to view is not visible on the screen, run a search for it.
3. The following information is provided for each collection:
   - Name, which can be clicked to view the list of documents in the collection. The range of actions you can take on each document varies, depending on the document type, but can include any combination of the following: append, insert, duplicate, or remove.
   - Total number of documents in the collection
   - Type of collection
   - Status of the collection
   - Activity log for the collection

## View the Activity Log for a Collection

1. Click and select **Provisioning** > **Collection**.
   The **Collection** screen opens, displaying all provisioning collections in the system.
2. If the collection whose activity log you want to view is not visible on the screen, run a search for it.
3. In the Activity Log column, click the link for the collection.
   The collection log screen opens, listing the date and log message for every activity carried out for the collection.




## Append a Collection

To append a collection in AppViewX:

1. Click and select **Provisioning** > **Collection**.
   The Collection screen opens.
2. Select the checkbox beside the collection you want to append.

3. Click  in the Command bar.
4. Make the required changes to the collection and click **Save**.

> **Note:** Click the Collection snapshot link to access a sample JSON object which can be used while creating collections.

## Download a Collection

To download a collection:

1. Click  and select **Provisioning** > **Collection**.
   The Collection screen opens.
2. Select the custom collection you want to download.
3. Click  in the Command bar.
4. Click **OK** on the Confirmation popup screen that appears.
   The selected custom collection is downloaded to your computer as an XLS file.

## Export a Collection

To export a collection:

1. Click  and select **Provisioning** > **Collection**.
   The Collection screen opens.
2. Select the collection you want to download.
3. Click  in the Command bar.
4. Click **OK** on the Confirmation popup screen that appears.
   The selected custom collection is downloaded to your computer as a zip file. If required, you can modify the contents and then import the collection back into the AppViewX system later on.

> **Note:** To export multiple collections at the same time, select the checkboxes for each of them.

## Import a Collection

To import a collection:

1. Click and select **Provisioning** > **Collection**.
   The Template screen opens.
2. Click in the Command bar.
3. On the Import screen that opens, click Browse and navigate to the file you want to import, then click Open.
4. On the Import screen, click **Upload**.
   If the file is valid it will be uploaded and displayed in the collection grid, along with one of the following statuses:
   - In progress
   - Completed
   - Failed

   **Note:**
5. The file you import must contain the following values: collection name, group by, order by, and unique key. If it does not, an error message appears when you click to upload your file.

## Modify a Collection

To modify a collection:

1. Click and select **Provisioning** > **Collection**.
   The **Collection** screen opens, displaying all collections in the system.
2. If the collection whose details you want to modify is not visible on the screen, run a search for it.
3. Click the collection name to open its details screen.
4. Click beside the component whose contents you want to modify.
5. Click **Update** to save your changes to the collection.

## Delete a Collection

To delete a collection:

1. Click and select **Provisioning** > **Collection**.
   The **Collection** screen opens.
2. If the collection you want to delete is not visible on the screen, run a search for it.
3. Select the checkbox beside the collection name.

4. Click  in the Command bar.
5. On the confirmation screen that pops up, click **OK**.

   The **Collection** screen refreshes and the collection no longer appear in the list or anywhere in the system.

# Chapter 7: Inventory



## Inventory Module

The Inventory module is the asset management system of AppViewX. It allows you to view and manage/ monitor the following:

- Devices
- Certificates
- SSH
- Group
- Backup & Restore

## Device Tasks

- Overview
- Add a Device
- Modify a Device
- Delete a Device
- Add a Credential to a Device
- Manage and Unmanage Devices
- Import Devices
- Export Device Details
- Manually Fetch the Configuration for a Device
- Generate and Download an iHealth Report

## Overview

The Device screen within the Inventory module allows you to perform the following inventory-related tasks for devices:

- Add a device
- Modify a device
- Delete a device
- Add a credential to a device
- Manage and unmanage devices
- Export device configurations
- Import device configurations
- Manually fetch a device configuration
- Generate and download an iHealth report

## Add a Device

Because a wide range of devices from different vendors can be added to the AppViewX system, it is not possible to explain the exact steps you must complete for each device type. The following instructions explain only the basic steps required. Refer to the AppViewX UI for the specific fields and configuration options relating to a particular device type.

To add a device to the AppViewX system:

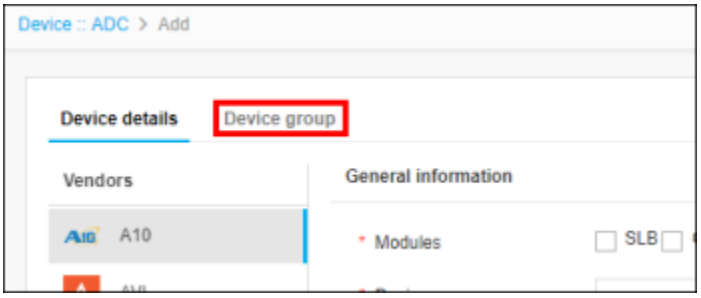
1. Click  and select **Inventory** > **Device**.
   The Device screen opens.
2. On the top of the screen, click the tab that corresponds to the type of device you want to add: ADC, server, DNS, firewall, WAF, switch, router, proxy, cloud, HSM, others, or MDM.

   **Note:**
   - To manage the Amazon ELB devices, ensure that the proxy is configured in the Settings module. For detailed information, refer to the Proxy Settingssection of this guide.
   - Servers should be added only with the root user credentials who can access all the files. Also, in the **Credentials** pane, users should select **sudo** or **dzdo** from the **Access Elevation** section.

3. Click  in the Command bar.

4. In the left-hand column on the Add screen that appears, select the vendor whose device you want to add.
5. At a minimum, fill in all fields that contain a red asterisk beside their names.
6. Click **Save**.

> **Note:** In some instances, such as when adding ADC devices, a second tab must be clicked and its fields completed before the device can be added to the AppViewX system. Before leaving the Add screen, check to see if there are additional tabs you need to click, like the Device group tab in the image below.




• Integrate an HSM Device

## Integrate an HSM Device

To integrate an HSM device in AppViewX:

1. Click ☰ and select **Inventory** > **Device**.
   The Device screen opens.
2. On the screen that appears, select the vendor and click + in the Command bar.
3. At a minimum, complete all fields designated with a red asterisk (*).The devices that are set to **Default** will be used for the private key encryption process.
4. Click **Save**.
5. If you want to edit the settings for a particular application, click that account. The fields corresponding to that account become editable.
6. Make whatever changes you want to the information on the screen, then click **Update**.

## Modify a Device

To modify a device, complete the following steps:

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to modify: ADC, server, DNS, firewall, WAF, switch, router, proxy, cloud, or others.
3. If the device is not visible on the screen, run a search for it.
4. Click the device name in the Name column.
5. Make whatever modifications you want to the device details.
6. Click **Save** to save your changes.

> **Note:** You can modify the details (such as FQDN, IP address, and the modules supported) only for the ADC device.

## Delete a Device

To delete a device from the AppViewX system:

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to delete: ADC, server, DNS, firewall, WAF, switch, router, proxy, cloud, or others.
3. If the device is not visible on the screen, run a search for it.
4. Click the checkbox beside the device name.
5. Click in the Command bar.
6. On the popup screen that appears, click **Yes** to confirm that you want to delete the device.
   The screen refreshes and the device no longer appear on the screen or anywhere in the AppViewX system.

## Add a Credential to a Device

You can create a credential for both the AppViewX and CyberArk sources.

- Add a Credential to AppViewX
- Add a Credential to CyberArk

## Add a Credential to AppViewX

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to add a credential to ADC, server, DNS, firewall, WAF, switch, router, proxy, or others.
3. Click in the Command bar.
4. On the screen that appears, click .
   The **Add Credential** screen opens by selecting the **AppViewX** sub-tab by default.
5. Enter a name for the credential to help the users identify it when adding a device.
6. Enter the username and password associated with the credential.
7. If a secondary credential password was created when the device was added to the system, thus allowing different levels of control over the credential, enter this password in the Secondary password field.
8. Click **Save**.
   The credential is then added to the table at the credential page. You can delete a credential, user name, or password by selecting the checkbox beside the credential name in the table and then clicking in the Command bar.

## Add a Credential to CyberArk

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to add a credential to ADC, server, DNS, firewall, WAF, switch, router, proxy, or others.
3. Click in the Command bar.
4. On the screen that appears, click .
   The **Add credential** screen opens by selecting the **AppViewX** sub-tab by default.
5. Click the **CyberArk** sub-tab in the left-hand column.
6. Enter a name for the credential to help the users identify it when adding a device.
7. Select the **Device**, **Amazon(AWS/ELB)**, or **Microsoft Azure** radio button based on whose credentials you want to retrieve from the CyberArk vault.
   The following fields may vary based on the type you selected.

- **Device**
  a. Enter the user name associated with the credential.
  b. In the **App ID** field, enter the reference ID that was provided by CyberArk for the corresponding application.
  c. From the **User type** dropdown list, select one of the following
    - **Internal** - The user that is created directly in the device
    - **External** - The user that is created in the Active directory
  d. Click **Save**.
- **Amazon (AWS/ELB)**
  a. Enter the user name associated with the credential.
  b. In the **App ID** field, enter the reference ID that was provided by CyberArk for the corresponding application.
  c. In the **AWS access key ID** field, enter the access key ID generated from the AWS management console.
  d. Click **Save**.

## Manage and Unmanage Devices

To manage or unmanage devices, complete the following steps:

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to start or stop managing: ADC, server, DNS, firewall, WAF, switch, router, or proxy.
3. 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 managed or unmanage a device that is not in a managed state, an error message appears at the top of the screen.

4. Click the checkbox beside the device name.
5. To start managing the device, click in the Command bar at the top of the screen. To stop managing a device, click .

## Import Devices

Although you can import the details of multiple *devices* at the same time, you can only import details of one kind of device during each import action. So, for example, you can import details of five ADCs from a single .csv file, but you cannot import details of 3 ADCs and 2 servers from a single file. You would need to import the ADC details first and then run a separate import for the server details.

In addition, when you click to import a specific device type, you must be on the corresponding Device tab in the Inventory. So, when importing ADC devices, you must click the Import button on the ADC tab; if you try importing ADC devices from the Server tab, an error message appears.

**Note:** The most efficient way to import device details is to download the sample import file that is available by clicking  in the Command bar of the Import screen, modify the contents, save it, and then import it into the system. This reduces the chance that error messages appear during the import process.

To import devices using a .csv file, complete the following steps:

1. Click  and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of devices you want to import: ADC, server, DNS, firewall, WAF, switch, router, or proxy.
3. Click  in the Command bar.
4. On the Import screen that appears, navigate to the location of the import file, then select it.
5. Click Import to add the devices and their details to the AppViewX inventory.

**Note:** AppViewX currently supports uploading up-to 60000 server details in a single upload file.

## Export Device Details

Although you can export the details of multiple *devices* at the same time, you can only export details of one kind of device during each export action. So, for example, you can export details of five ADCs to a single external file, but you cannot export details of 3 ADCs and 2 servers to a single file. You would need to export the ADC details first and then run a separate export for the server details.

To export the details of one or more devices:

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to export: ADC, server, DNS, firewall, WAF, switch, router, proxy, or others.
3. If the device you want to export is not listed on the screen, run a search to locate it.
4. 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.
5. Click in the Command bar at the top of the screen.
6. 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 AppViewX inventory.
7. On the screen that opens, select the location where you want the device details file to go, then click Save.
   The details are then downloaded as an Excel.xls file.

## Manually Fetch the Configuration for a Device

To manually get the configuration for a device:

1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. At the top of the screen, click the tab that corresponds to the type of device you want to fetch a configuration for: ADC, server, DNS, firewall, WAF, switch, router, or proxy.
3. If the device is not listed on the screen, run a search to locate it.
4. Click the checkbox beside the device name. If you want to fetch configurations for multiple devices of the same type, select their checkboxes, too.
5. Click in the Command bar.
   A notification appears at the top of the screen stating, "Fetch config has been triggered for the device(s)."

> **Note:** You cannot fetch configurations for different device types - ADCs and firewalls, for example at the same time. These actions must be performed separately.

## 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 only 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 Settingssection of this guide.

To generate and download an iHealth report:

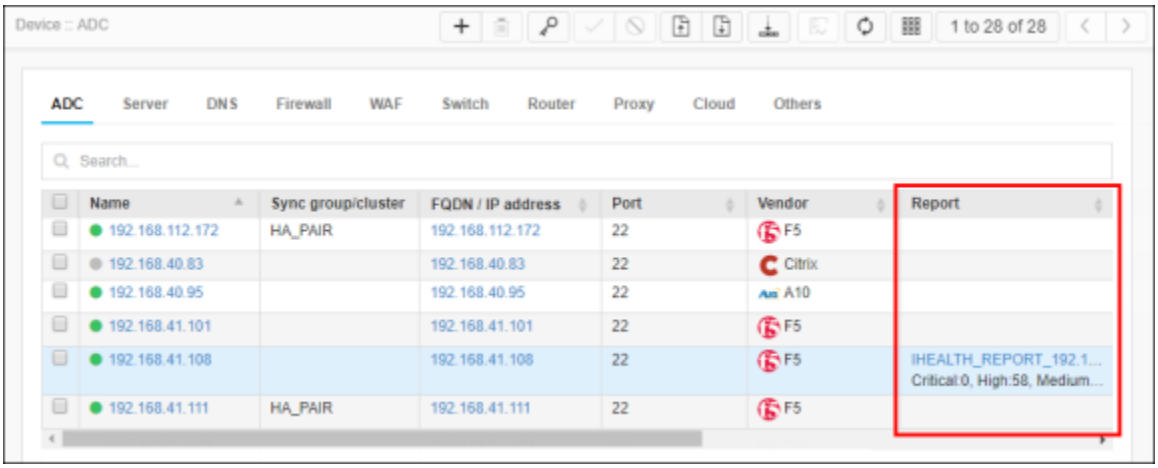
1. Click and select **Inventory** > **Device**.
   The Device screen opens.
2. Select the checkbox beside the ADC device for which you want to generate an iHealth report.
3. Click in the Command bar.

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

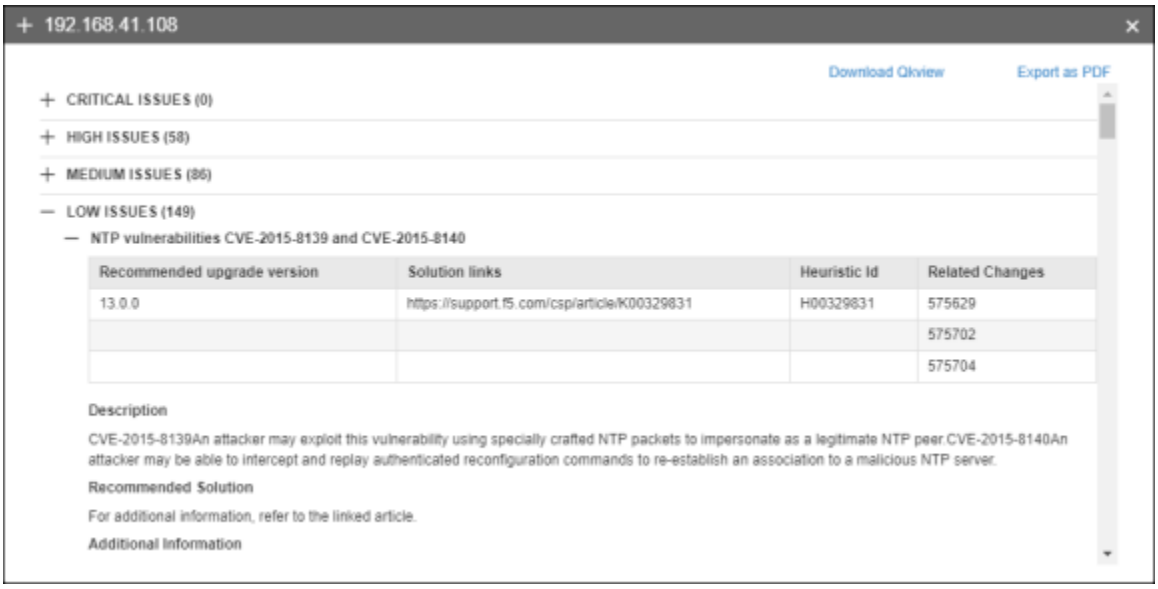
4. On the iHealth Report Generate screen that pops up, enter the case number for the report, then click Generate.

   **Note:** When the report is generated, it appears as a link in the Report column on the Device: ADC screen.

5. Click the **IHEALTH_REPORT** link.
   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.




6. Click + beside a severity level to view the issues within the corresponding category.
   Within each severity level, click the name of a specific issue to view complete details, a recommended solution, and additional information about it.




**Note:** (Optional) Download the entire iHealth report as a Qkview file in 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.

# Certificate Tasks

- Certificate Tasks Overview
- Managing Certificates

- Discover a Certificate
- Discover a Certificate: IP Range
- Discover a Certificate: Subnet
- Discover a Certificate: URL
- Discover a Certificate: Upload
- Discover a Certificate: Managed ADCs
- Discover a Certificate: Managed Servers
- Discover a Certificate: Managed MDMs
- Discover a Certificate: Certificate Authority
- Discover a Certificate: Managed Firewalls
- Discover a Certificate: Managed WAFs
- Discover a Certificate: Clouds
- Rediscover a Certificate
- Abort Certificate Discovery
- Schedule a Certificate Discovery
- View Certificate Topology
- Add an Application Connector to a Server Certificate Topology
- Add an Application Connector to a Client Certificate Topology
- Add a Certificate Authority Connector to a Certificate Topology
- Enroll a Certificate
- Enroll a Code Signing Certificate
- Push a Certificate to a Device
- Renew a Certificate
- Regenerate a Certificate
- Reissue a Certificate
- Revoke a Certificate
- Suspend Certificate
- Reinstate a Certificate
- Add/Modify Comments
- Perform Revocation Check
- Roll Back a Certificate from a Device
- Delete a Certificate
- Generate a CSR for a Certificate

- Submit a CSR to a Certificate Authority
- Download a CSR for a Certificate
- Assign or Unassign a Group to a Certificate
- Change the Status of a Certificate
- Upload a Certificate
- Download a Certificate
- Export Inventory Data of a Certificate
- Upload a Certificate Key
- Download a Certificate Key
- Run SSL Checker on a Certificate
- Add or Modify a Certificate Authority Account
- Configure a Custom Certificate Authority
- Add a Programmable Application Connector
- Add a Password in the Vault
- Configure the Job Scheduler
- Configure General Certificate Settings
- Configure Auto-Enrollment Settings
- Configure a Programmable Certificate Authority
- Configure a Known Certificate Authority
- Create a Root and Intermediate Certificate Authority
- Create a CA Policy
- View the Process Explorer

## Certificate Tasks Overview

The widgets in the dashboards contain reports that provide consolidated statistics for the list of all accessible certificates by extracting its data from the certificate inventory and record the key value indicators for expiry and compliance use cases.

- To view samples of each of the reports listed in this topic, refer to Appendix B, Sample Certificate Reports.
- Click on the legends to select/deselect the data that you want to be displayed/hid respectively on the chart.
- Except for the Cipher Suite Report, when you click on any sector/bar of the chart, an Inventory screen appears displaying the certificate details corresponding to the sector/bar you clicked.

- Server Certificate
- Client Certificate
- Code Signing Certificate
- Server Certificate Security
- Client Certificate Security
- Server Endpoint Security
- Client Endpoint Security
- Server Standard Dashboard
- Client Standard Dashboard
- SSL Validation Report

## Server Certificate

To view the widgets related to server certificate:

1. Click  and select **Dashboard**.
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 **Server Certificate**.
5. Although each report displays the data differently, the same set of data is used to generate each report.
6. The following reports are segregated and displayed as widgets on the **Server Certificate** screen:
   - **Report by Certificate Authority** - A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
     - Green - Valid certificates
     - Blue - Certificates with an expiry in 90 days
     - Yellow - Certificates with expiry in 30 days
     - Orange - Certificates with expiry in 10 days
     - Red - Expired certificates

  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month** - A bar chart that shows the total number of certificates expiring each month.
- **Validation Status** - A doughnut chart that shows the number of certificates residing in the host environment or residing within our AppViewX Certificate Inventory, with each sector displaying the number of trusted, non-trusted, and unverified certificates.
- You can perform the following actions from the Validation Status widget:
  - Export a report
  - Configure a report settings
- **Policy Compliance Report** - A pie chart that shows the number of compliant and non-compliant certificates in the system, with each sector in the chart representing a different kind of policy such as Strict or Suggestive. Also, you can export the report details from the Policy Compliance Report widget.
- **Report by Source** - A bar chart that shows the total certificate count against the source (point of deployment), made up of colored bars representing the same statuses listed for the Report by Certificate Authority widget.
- **Orphan Certificate Report** - A bar chart that displays the following details:
  - Certificates that are not pushed to any device for more than 90 days. The count is collected when the connector is not in sync with that particular certificate.
  - Certificates that are dissociated from the profile being pushed to the device.
  - Certificates that are deleted manually from its location being pushed to the device.
- **Stale Certificate Report** - A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary Report** - A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the Report by Certificate Authority widget. You can also configure the report settingsfrom the Certificate Summary Report widget.
- **Count by Issuer** - A doughnut chart that shows the total number of certificates managed by the issuer such as Root CA or the Intermediate CA. You can also configure the report settingsfrom the Count by Issuer widget.
- **Cipher Suite Report** - A bar chart that categorizes the number of certificates against the supported ciphers suites, based on their strength. The cipher suite report with cipher strength "High" is displayed by default. You can select "Medium" or "Low" to view the respective reports.

## Client Certificate

To view client certificate reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Client Certificate**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Client certificate** screen:

- **Report by Certificate Authority** - A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month** - A bar chart that shows the total number of certificates expiring each month.
- **Policy Compliance** - A pie chart that shows the number of compliant and non-compliant certificates in the system, with each sector in the chart representing a different kind of policy such as Strict or Suggestive. You can also export the report details from the Policy Compliance Report widget.
- **Stale Certificate** - A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary** - A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the Report by Certificate Authority widget. You can also configure the report settings from the Certificate Summary Report widget.
- **Count by Issuer** - A doughnut chart that shows the total number of certificates managed by the issuer such as Root CA or the Intermediate CA. You can also configure the report settings from the Count by Issuer widget.

## Code Signing Certificate

To view codesigning certificate reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.

3. In the dropdown list that appears, click **CodeSigning Certificate**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **CodeSigning Certificate** screen:

- **Report by Certificate Authority** - A bar chart that shows the total certificate count for each Certificate Authority (CA), made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates
- **Expiry Report by Month** - A bar chart that shows the total number of certificates expiring each month.**Stale Certificate** - A pie chart that shows the number of expired and revoked certificates.
- **Certificate Summary** - A doughnut chart that categorizes the certificates based on expiration, with the total count of certificates made up of colored bars representing the same statuses listed for the Report by Certificate Authority widget. You can also configure the report settings from the Certificate Summary Report widget.

## Server Certificate Security

To view server certificate security reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Server Certificate Security**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Server Certificate Security** screen:

- **Certificate Transparency** - A metric chart that shows the count of domains for which there are some unmanaged certificates in AppViewX.
- **CAA Record** - A pie chart that shows the count of server certificates in AppViewX inventory, which have and do not have the CAA record. When the graph is clicked, AppViewX will display the server inventory with the list of its respective certificates.
- **Key Algorithm** - A bar chart that shows the count of server certificates enrolled with different key algorithms and sizes for encryption and decryption. When the graph is clicked, AppViewX will display the common name, issue name, and CAA status.
- **Hash Algorithm** - A bar chart that shows the count of server certificates enrolled with the different types of content cryptographic hashing algorithm details. When the graph is clicked, AppViewX will display the server inventory with the list of its respective certificates.

## Client Certificate Security

To view client certificate security reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Client Certificate Security**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Client Certificate Security** screen:

- **Certificate Transparency** - A metric chart that shows the count of domains for which there are some unmanaged certificates in AppViewX.
- **CAA Record** - A pie chart that shows the count of client certificates in AppViewX inventory, which have and do not have the CAA record. When the graph is clicked, AppViewX will display the client inventory with the list of its respective certificates.
- **Key Algorithm** - A bar chart that shows the count of client certificates enrolled with different key algorithms and sizes for encryption and decryption. When the graph is clicked, AppViewX will display the common name, issue name, and CAA status.
- **Hash Algorithm** - A bar chart that shows the count of client certificates enrolled with the different types of content cryptographic hashing algorithm details. When the graph is clicked, AppViewX will display the server inventory with the list of its respective certificates.

## Server Endpoint Security

To view server endpoint security reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Server Endpoint Security**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Server Endpoint Security** screen:

- **Certificate Monitor Statuses** - A pie chart that shows the sync status for the count of server certificates pushed from AppViewX. The following sync status is shown: Not synchronized, Synchronized, Deleted, and Not associated. On click of a count in the report, AppViewX will display a tabular column report in which the following details will be shown: certificate common name, device profile name, connector type, vendor name, device name, and sync status.
- **TLS Version** - A grid that shows the count of server certificates with respect to the TLS versions. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Cipher Suite** - A pie chart that shows the count of server certificates with respect to the cipher suite details along with the cipher suite priorities. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Heartbleed Poodle** - A grid that shows the count of device endpoints that are exposed to heartbleed vulnerabilities. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Certificate Auto Push** - A pie chart that shows the count of server certificate device connectors configured and not configured with the push automatically feature.

## Client Endpoint Security

To view client endpoint security reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Client Endpoint Security**.

> **Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Client Endpoint Security** screen:

- **Certificate Monitor Statuses** - A pie chart that shows the sync status for the count of server certificates pushed from AppViewX. The following sync status is shown: Not synchronized, Synchronized, Deleted, and Not associated. On click of a count in the report, AppViewX will display a tabular column report in which the following details will be shown: certificate common name, device profile name, connector type, vendor name, device name, and sync status.
- **TLS Version** - A grid that shows the count of server certificates with respect to the TLS versions. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Cipher Suite** - A pie chart that shows the count of server certificates with respect to the cipher suite details along with the cipher suite priorities. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Heartbleed Poodle** - A grid that shows the count of device endpoints that are exposed to heartbleed vulnerabilities. On click of the count in the report, AppViewX will display a tabular column report in which the following details will be shown: common name, partition, port, vendor, profile, host, category, and device name.
- **Certificate Auto Push** - A pie chart that shows the count of server certificate device connectors configured and not configured with the push automatically feature.

## Server Standard Dashboard

To view server standard dashboard reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Server Standard Dashboard**.

**Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Server Standard Dashboard** screen:

- **Certificate Discovery Trend** - A line chart that shows the trend of certificates discovered in AppViewX in the last 30 days.
- **Certificate Auto-Renewal Readiness** - A pie chart that shows the count of auto-renewal enabled certificates, which are ready for the auto-renewal process.
- **Certificate CA Actions** - A grid that shows the count of CA actions performed based on the certificate groups.
- **Report by Certificate Authority Account - Server** - A bar chart that shows the total certificate count for each Certificate Authority (CA) Account, made up of colored bars representing the following statuses:
  - Green - Valid certificates
  - Blue - Certificates with an expiry in 90 days
  - Yellow - Certificates with expiry in 30 days
  - Orange - Certificates with expiry in 10 days
  - Red - Expired certificates
  - Black - Revoked certificates
  - Gray - New certificates

## Client Standard Dashboard

To view client standard dashboard reports:

1. Move your cursor to the breadcrumbs field of the current dashboard.
2. Click the current dashboard name.
3. In the dropdown list that appears, click **Client Standard Dashboard**.

**Note:** Although each Client certificate report displays the data differently, the same set of data is used to generate each report.

The following reports are segregated and displayed as widgets on the **Client Standard Dashboard** screen:

- **Certificate Discovery Trend** - A line chart that shows the trend of certificates discovered in AppViewX in the last 30 days.
- **Certificate Auto-Renewal Readiness** - A pie chart that shows the count of auto-renewal enabled certificates, which are ready for the auto-renewal process.
- **Certificate CA Actions** - A grid that shows the count of CA actions performed based on the certificate groups.

## SSL Validation Report

To view the widgets related to SSL Validation Report:

1. Click  and select **Dashboard**.
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 **SSL Validation Report**.

   The following reports are segregated and displayed as widgets on the **SSL Validation Report** screen:
   - **Vulnerability Report** A grid that shows the count of device endpoints that are exposed to Heartbleed, ROCA, and Poodle vulnerabilities.
   - **Cipher Suites** A grid that shows the count of client certificates with respect to the cipher suite details along with the cipher suite priorities.
   - **TLS version** grid that shows the count of client certificates with respect to the TLS versions.
   - **Hash Algorithm** A pane that shows the count of certificates enrolled with the different types of content cryptographic hashing algorithm details.
   - **CAA Record** A pane that validates and provides the Certificate authority and authorization record value for the end certificates.
   - **Key Type**A pane that shows the key algorithms and sizes for encryption and decryption of the enrolled certificates.
   - **CERT Status**It shows the complete certificate life-chain (root, intermediate, and end).
   - **Summary** pane displays a table with the certificate strength and a score-meter that denotes the credibility of the certificate.

## Managing Certificates

Certificate Management is a one-stop solution that allows you to monitor and manage all the SSL (Secure Sockets Layer) certificates installed within an organization. This includes Application servers, Web servers, and Application Delivery Controllers (ADCs). The certificates and their keys are essential to identify the authenticity of a website and to encrypt the data sent to the server.

In AppViewX, Certificate Management provides the following capabilities:

- Automatically discover the SSL certificates within the network of an organization.
- Monitors the validity of all the SSL certificates and alert you through email or SNMP trap before the certificate expires.
- Allows certificate management actions such as creating a new certificate, renewing certificates, and revoking certificates.
- Role-Based Access Control (RBAC) allows you to create a customized role to perform selective actions on certificates.
- Provides visibility of a holistic view of a certificate with complete information about the certificate.
- Allows policy-driven compliance check and certificate enrolment action in a single console without manual intervention.
- Ability to migrate to the recommended standards such as SHA-1 or SHA-2.

## Certificate Lifecycle Automation using Visual Workflow

Workflow is used for selective restriction of work order approval and implementation with either Read or Read/Write permission. Based on the workflow associated, a user can Approve, Implement, Reject, or Discard a work order. Visual workflow allows the user to automate & orchestrate the certificate lifecycle. It provides the capability to define a custom business process based on the organization's needs. It allows for having a custom workflow approval process as part of the automation process. Users must be assigned with privileges to the workflow templates in a Certificate based on the role assigned.

AppViewX provides pre-built out of the box workflows to automate the certificate lifecycle process to perform:

- Bulk_Cert_Renewal_Implementation
- Cert_Generation_Implementation
- Cert_Push_implementation
- Cert_Renewal_Implementation
- Cert_Revocation
- Cert_Rollback_implement

The Certificate screen within the Inventory module allows you to perform the following inventory-related tasks for server and client certificates:

- Discover a certificate
- View certificate topologies

- Add different kinds of connectors to client and server certificate topologies
- Create a certificate
- Push a certificate to a device
- Renew a certificate
- Reissue a certificate
- Regenerate a certificate
- Revoke a certificate
- Rollback a certificate
- Generate a CSR (server certificates only)
- Submit a CSR to a Certificate Authority
- Download a CSR for a certificate
- Assign or unassign a group to a certificate
- Change the status of a certificate
- Upload a certificate
- Download a certificate(server certificates only)
- Export a certificate
- Upload a certificate key
- Download a certificate key
- Configure certificate settings
- Delete a certificate
- Run SSL checker on a certificate(server certificates only)
- Create a certificate group
- View and edit the system settings for each of the server vendors
- Configure a Programmable Certificate Authority

For Device certificates, you can perform the following tasks:

- Export a certificate
- Download a certificate
- Renew a certificate
- Reissue a certificate
- Regenerate a certificate
- Revoke a certificate
- Delete a Certificate
- Assign or unassign a group to a certificate
- Create a certificate group

For Policy, you can perform the following two tasks:

- Create a policy
- Delete a policy

For Intermediate and Root certificates, you can only perform the following task:

- Download a certificate

## Discover a Certificate

Discover function allows you to search and display the list of available certificates within an organizational network to manage it in the AppViewX certificate inventory.

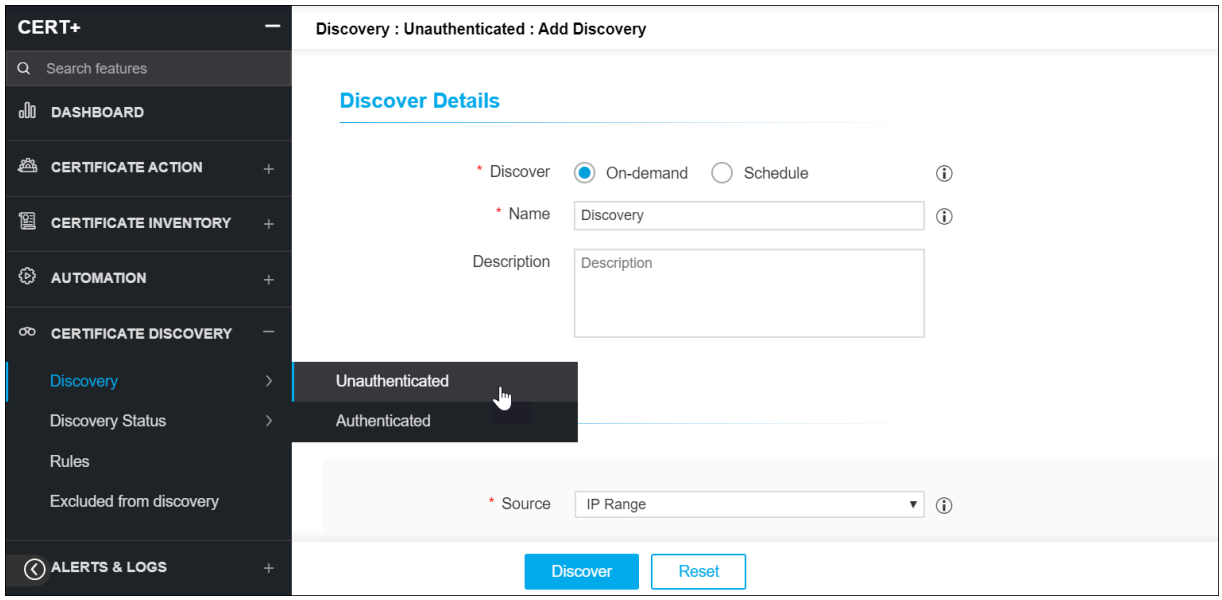
You can initiate a discovery on-demand or you can schedule as required. To initiate an authenticated or unauthenticated discovery:

1. Click  and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated** or **Authenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select**On-demand**or **Schedule** . On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.
4. You can also upload the following details to the template in the .csv, .xls, or .xlsx format.
5. Enter the **Discovery Name** and **Description** in the respective fields.
6. Under the **Discover By** section, in the **Source** field, select one of the following details.

> **Note:** You can discover certificates from a wide range of sources like IP, Subnet, URL, Managed Devices, Managed Servers, Managed MDMs, Managed Firewalls, Managed WAF, Clouds, and Certificate Authorities.

The following are the details that have to be entered as per the source:

> **Note:** For **Unauthenticated Discovery**, you can discover certificates from a wide range of sources like IP, Subnet, URL, and Upload option. For **Authenticated Discovery**, you can discover certificates from a wide range of sources like Managed Devices, Managed Servers, Managed MDMs, Managed Firewalls, Managed WAF, Clouds, and Certificate Authorities.




- **IP Range**
  - **Start IP:** You can enter an IPv4 lesser than End IP.
  - **End IP:** You can enter an IPv4 greater than Start IP.
  - **IP Split Level:** Based on this value, the provided range of IP addresses will be split into multiple batches for the discovery process.
  - **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (Eg. 444-666,888-999,922,44). You can also select **All ports** to include port numbers from 0 to 65535.
  - **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
  - **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.
  - **Scan Type:** There are two scan types in this option:
    - Aggressive: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
    - Passive: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.
  - **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

- **Subnet**
  - **Network:** You can enter the network details in this field.
  - **Subnet Split Level:** Based on this value, the provided subnet will be split into multiple batches for the discovery process.
  - **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (Eg. 444-666,888-999,922,44). You can also select **All ports** to include port numbers from 0 to 65535.
  - **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
  - **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.
  - **Scan Type:** There are two scan types in this option:
    - Aggressive: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
    - Passive: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.
  - **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.
- **URL**
  - **URL:** You can enter the URL in this field.
  - **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (Eg. 444-666,888-999,922,44). You can also select **All ports** to include port numbers from 0 to 65535.
  - **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
  - **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.
  - **Scan Type:** There are two scan types in this option:
    - Aggressive: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
    - Passive: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.

- **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
  - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
  - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.
- **Upload**
  - **Choose File:** You can upload any of the following file types : .crt, .cer, .der, .p7b, .p7c, .pem, .pfx, .jks, .zip, .tar, .tar.gz, .p12 file.
  - **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.
- **Managed ADCs**
  - Select the list of devices and click **Add as favorites**.
  - **Batch Execution Type:** You can run multiple batches in parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.
  - **Discovery Type**: You can choose between all certificates or certificates in use. Either all certificates or only the associated certificates with endpoints will be discovered.
- **Managed Servers**
  - Select the list of devices and click **Add as favorites**.
  - **Batch Execution Type:** You can run multiple batches in parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

- **Discovery Type:**: You can choose between all certificates or certificates in use. Either all the certificates or only the associated certificates with the endpoints will be discovered.
- **Directories to Scan:** You can choose between Default and Custom. Certificates can be discovered from the default or the customized directory defined by the user. Default directories are obtained through server config fetch.

- **Managed MDMs, Managed Firewalls, Managed WAF, Clouds, and Certificate Authorities**
  - Select the list of devices and click **Add as favorites**.
  - **Batch Execution Type:** You can run multiple batches in parallel or sequentially. You can choose between parallel and sequential execution.
    - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
    - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

Apache is the currently supported vendor for this feature.

7. Under **Discovery Rules**, in the **Associate Rule** field, you can **Select the Associate Rule** option from the drop-down. Rules created through the **Rules** inventory inside the discovery module will be listed. Based on the selection, conditions will be applied to discovered certificates.
8. Under **After Discover** section, in the **Move Certificate to Inventory with Status** field:
   You can select between the following options:
   - **Do not move:** Newly discovered certificates and its objects will not be moved to the inventory.
   - **Managed:** Newly discovered certificates and its objects will be moved to the inventory with Managed status.
   - **Monitored:** Newly discovered certificates and its objects will be moved to inventory with the Monitor status.

   If the discovered certificate already exists in the inventory, its objects will be moved with the same status.
9. In the **Certificate Group** field, select a certificate group from the drop-down. Discovered certificates will be associated with the provided certificate group. Based on the group association, the policy will also be applied to these certificates to check compliance.

**Note:** You can discover any encrypted certificate/key by updating the **Password Vault**.

10. For **Scheduled Discovery**, under the **Discover Details** section, select **Schedule**.
11. Enter the **Discovery Name** and **Description** in the respective fields.

- **Occurrence Type:** You can select the frequency of the discovery process in this section. You can choose between Daily, Weekly, Monthly, and Yearly.
- **Starts On:** You can select the start date and time for the discovery process in this field.
- **Ends:** In this section, you can choose between the following:
  - **Never:** You can select this option if you never want the discovery process to end.
  - **After** a specific number of occurrences: You can enter the number of occurrences after which you want the discovery process to stop in this field.
  - **On:** You can enter the date by when you want to end the discovery process.

12. Follow steps from 6 to 9.

## Discover a Certificate: IP Range

To discover a certificate by IP range:

1. Click  and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

**Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **IP Range** from the dropdown.
6. **Start IP:** You can enter an IPv4 lesser than End IP.
7. **End IP:** You can enter an IPv4 greater than Start IP.
8. **IP Split Level:** Based on this value, the provided range of IP addresses will be split into multiple batches for the discovery process.
9. **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (For example, 444-666, 888-999, 922, 44). You can also select **All Ports** to include port numbers from 0 to 65535.
10. **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
    **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.

- **Scan Type:** There are two scan types in this option:
  - **Aggressive**: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
  - **Passive**: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.
- **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
  - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
  - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

## Discover a Certificate: Subnet

To discover a certificate by subnet:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

   **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Subnet** from the dropdown.
6. **Network:** You can enter the network details in this field.
7. **Subnet Split Level:** Based on this value, the provided subnet will be split into multiple batches for the discovery process.
8. **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (For example, 444-666, 888-999, 922, 44). You can also select **All Ports** to include port numbers from 0 to 65535.
9. **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
   **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.

- **Scan Type:** There are two scan types in this option:
  - **Aggressive**: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
  - **Passive**: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.
- **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
  - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
  - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

## Discover a Certificate: URL

To discover a certificate by URL:

1. Click  and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

    **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **URL** from the dropdown.
6. **URL:** You can enter the URL in this field.
7. **Ports:** You can enter any port number from 0 to 65535. You can separate port ranges with a hyphen (For example, 444-666, 888-999, 922, 44). You can also select **All Ports** to include port numbers from 0 to 65535.
8. **Datacenter (of AppViewX agent):** You can select the datacenter of the AppViewX agent from this drop-down list.
   **SNI Hostname(s):** AppViewX will discover the certificates based on the hostnames against the IP address. Multiple hostname values are supported by using the comma (,) as a delimiter.

- **Scan Type:** There are two scan types in this option:
  - **Aggressive**: AppViewX will discover the certificates from all IPs and ports based on the provided values, irrespective of the previous discovery details.
  - **Passive**: AppViewX will discover the certificates only from the IPs and ports from which the certificates are discovered previously.
- **Batch Execution Type:** Multiple batches will be run either parallel or sequentially. You can choose between parallel and sequential execution.
  - **Sequential Execution:** AppViewX will take and execute the batches one by one. The interval between the batches can also be defined.
  - **Parallel Execution:** AppViewX will take the number of batches based on the infrastructure capability and the discovery process will be executed for those number of batches in parallel.

## Discover a Certificate: Upload

To discover a certificate by upload:

1. Click  and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

**Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Upload** from the dropdown.
6. In the **Choose File** field, click **Upload** and go to the certificate you want to upload into the system, then click **Open**.

**Note:** You can upload any of the following file types: .crt, .cer, .der, .p7b, .p7c, .pem, .pfx, .jks, .zip, .tar, .tar.gz, .p12 file.

7. To upload certificates in bulk, you can create a **.zip**, **.tar**, or **tar.gz** file containing all the certificates and then click upload. You can upload any of the following file types in the **.zip**, **.tar**, or **tar.gz** file: .crt, .cer, .der, .p7b, .p7c, .pem, .pfx, .jks, .p12.

> **Note:** You can also upload encrypted keys in the **.zip**, **.tar**, or **tar.gz** file.

## Discover a Certificate: Managed ADCs

### Prerequisites

To discover certificates from managed ADCs, the ADC device should be managed under the AppViewX Inventory.

To discover a certificate:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Managed ADCs** from the dropdown. A list of managed ADC devices is displayed in the **Available Devices** field.
6. Select the device from which you want the certificates to be discovered.
7. Select the **Discovery Type** that must be used.

## Discover a Certificate: Managed Servers

### Prerequisites

To discover certificates from managed servers, the server device should be managed under the AppViewX Inventory.

To discover a certificate:

1. Click and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Managed Servers** from the dropdown. A list of managed servers is displayed in the **Available Servers** field. Select the server from which you want the certificates to be discovered.
6. Select the **Discovery Type** that must be used.
7. Select the **Default** or **Custom** directory to be scanned during the discovery.

## Discover a Certificate: Managed MDMs

### Prerequisites

To discover certificates from managed MDMs, the MDM device should be managed under the AppViewX Inventory.

To discover a certificate:

1. Click and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Managed MDMs** from the dropdown. A list of managed MDMs is displayed. Select the MDM from which you want the certificates to be discovered.

## Discover a Certificate: Certificate Authority

## Prerequisites

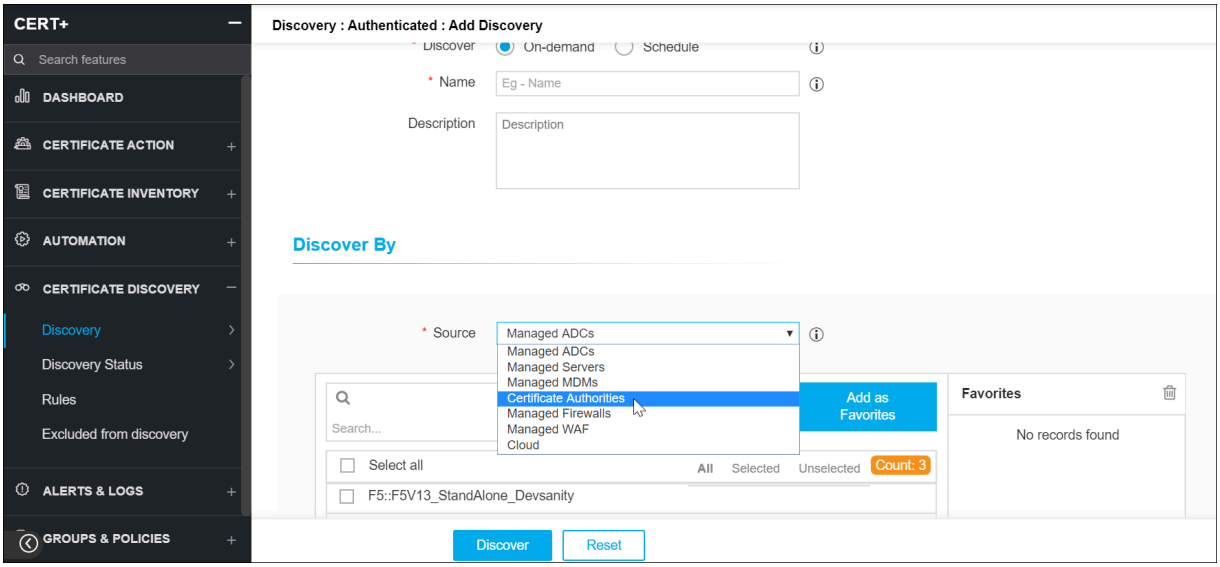
To discover certificates from a CA, the CA account should be determined under the AppViewX Inventory settings.

To discover a certificate:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Certificate Authorities** from the dropdown. A list of certificate authorities will be displayed in the **Available Certificate Authorities** field.
6. Select the Certificate Authority from which you want the certificates to be discovered.




> **Note:** For EJBCA, the revoked certificates are not discovered. On discovery, the end certs are discovered based on the days configured in the CA settings, the expired certificates are always discovered. The expiry days calculate from 0 - given value, for example, 0 - 1500.

On discovery, all the root and intermediate certificates that expire before 100 years will be discovered along with the end certificates by default. The discovered certificate count cannot be validated against the certificates present in the CA.

## Discover a Certificate: Managed Firewalls

### Prerequisites

To discover certificates from managed firewalls, the firewall device should be managed under the AppViewX Inventory.

To discover a certificate:

1. Click and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**. On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

   **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Managed Firewalls** from the dropdown. A list of managed firewall devices is displayed in the **Available Devices** field. Select the firewall device from which you want the certificates to be discovered.

## Discover a Certificate: Managed WAFs

### Prerequisites

To discover certificates from managed WAFs, the WAF device should be managed under the AppViewX Inventory.

To discover a certificate:

1. Click and select **CERT+** > **Certificate Discovery**.
2. Under Certificate Discovery, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**.

On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Managed WAF** from the dropdown.
   A list of managed WAF devices is displayed. Select the WAF device from which you want the certificates to be discovered.

## Discover a Certificate: Clouds

### Prerequisites

To discover certificates from a cloud, the cloud account should be determined under the AppViewX Inventory settings.

To discover a certificate:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under **Certificate Discovery**, click **Discovery** and select **Unauthenticated**.
3. On the **Add Discovery** page, under the **Discover Details** section, select **On-demand** or **Schedule**.
   On selecting **On-demand** discovery, AppViewX will trigger the discovery certificates process for that instance.

> **Note:** You can also upload the following details to the template in the .csv, .xls, or .xlsx format.

4. Enter the **Discovery Name** and **Description** in the respective fields.
5. Under the **Discover By** section, in the **Source** field, select **Cloud** from the dropdown.
   A list of cloud instances is displayed.
6. Select the cloud instance from which you want the certificates to be discovered.

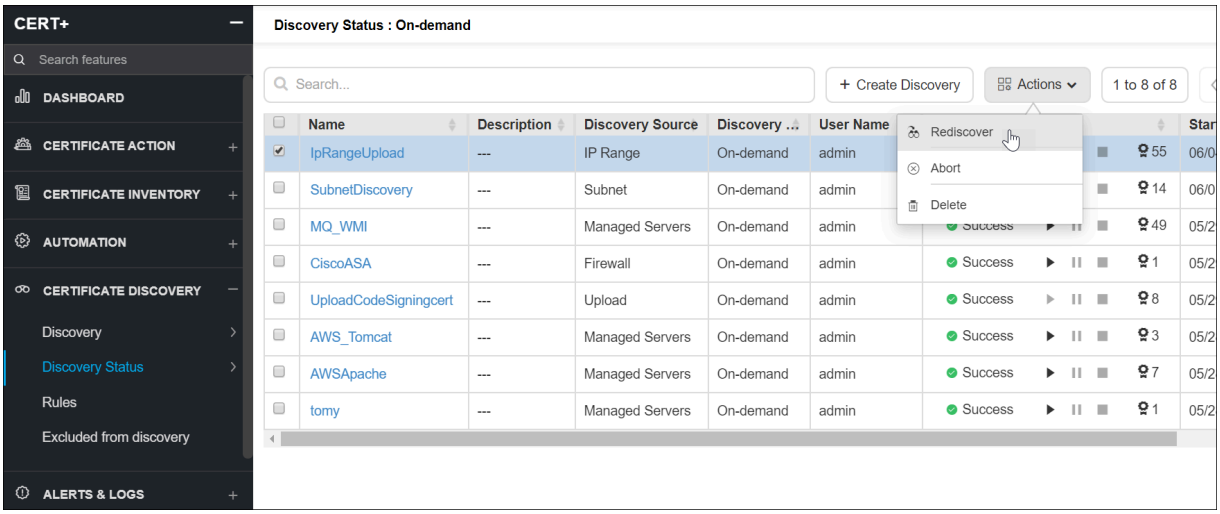
## Rediscover a Certificate

To rediscover a certificate:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under **Certificate Discovery**, click **Discovery Status** and select **On-demand** or **Scheduled**.
3. On the **Discovery Status** list view, select a certificate you want to rediscover.

4. Click **Actions** and select **Rediscover**.

   You can track the progress or status of rediscovery action in the **Discovery Status** column.

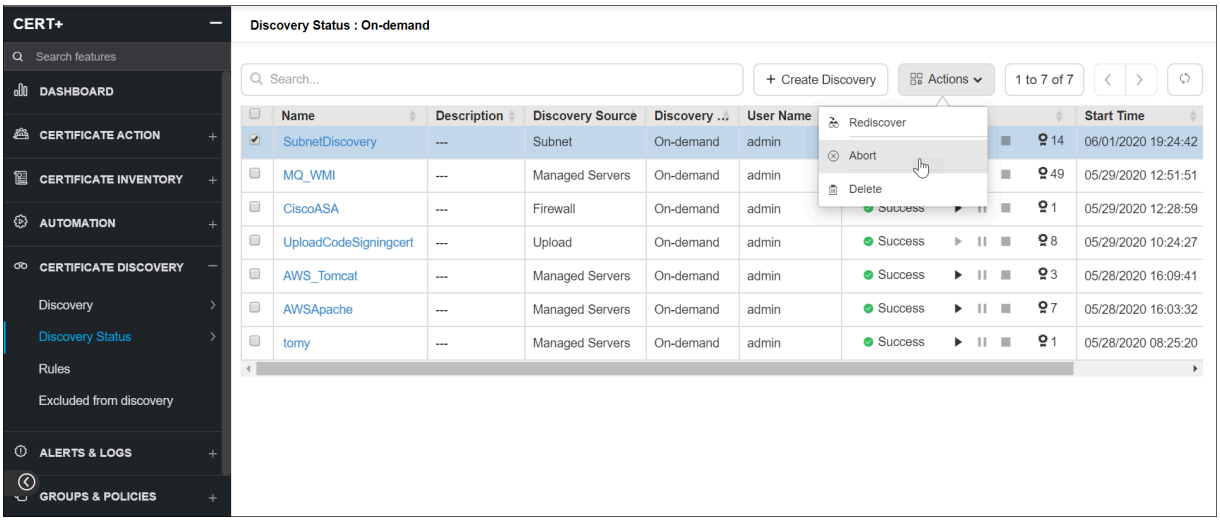



## Abort Certificate Discovery

To abort the certificate discovery process:

1. Click ☰ and select **CERT+** > **Certificate Discovery**.
2. Under **Certificate Discovery**, click **Discovery Status**.
3. On the Discovery Status list view, select a certificate discovery you want to abort.
4. Click **Actions** and select **Abort**.

   You can track the progress or status of the abort action in the **Discovery Status** column.



## Schedule a Certificate Discovery

The Scheduler function allows you to search and display the list of certificates at the time specified in the schedule.

To schedule a certificate discovery:

1. Click  and select **Inventory** > **Certificate**.
   The Certificate list view is displayed with the Server tab selected by default.
2. Click  on the top of the page.
3. On the **Discovery** screen, click **Scheduler**.
4. Click Schedule in the middle of the page or click  on the top of the page.

   **Note:** All certificates excluded from the discovery wull be visible in the **Excluded from Discovery** tab. Click  or  on the top of the page to move the selected certificate(s) to **Monitored** or **Managed** status respectively in the Certificate inventory. Also, you can click  to remove certificates from the exclusion list and make them available during discovery.

   The Add Discovery page is displayed with the Schedule radio button selected by default.
5. In the **Name** field, enter a name that identifies the certificate discovery action.
6. In the **Description** field, enter a description of the key discovery that makes it easy for a reader to determine when the key discovery is scheduled to take place.
7. From the **Occurrence type** dropdown, select the frequency for the certificate discovery process: daily, weekly, monthly, or yearly. Other fields in the Scheduler section populate depending on the selection.

   **Note:** Fields with a red asterisk (*) are mandatory.

8. In the **.** field, select a method to discover certificates:
   - IP range
   - Subnet
   - URL
   - Uplaod
   - Manage ADCs
   - Manage MDMs
   - Manage WAF
   - Manage Servers

- Certificate Authorities
- Clouds

9. From the **Certificate Group** dropdown, select a group to associate discovered certificates.

> **Note:** The time and date fields displayed next will depend on the selected option. For recurring discoveries, select the start and end date you want key discovery to begin and end respectively.

10. Depending on the status of certificates displayed in the inventory, you can select:
    - **Do not move**
    - **Managed**(You can perform actions (Create, Renew, Revoke) on those certificates)
    - **Monitored**((For alerting purposes, you will not be able to perform any actions on the certificates)
11. To exclude the certificate from the list of discovered certificates, select the checkbox next to **Compare certificate(s) with "Exclude from discovery" list and ignore**.
12. Enter template names of the Microsoft CA issued certificates, that you do not want to be discovered.
13. Click **Schedule**.

## View Certificate Topology

To view the topology that a server or client certificate belongs to,

1. Click and select **CERT+** > **Certificate Discovery**.
2. Under **Certificate Inventory**, click **Server** or **Client** .
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate for which you want to view the topology.
   The screen refreshes and displays the topology of the corresponding certificate.

The certificate with history is denoted by an **H** symbol beside its name (applicable only for certificates that are reissued, renewed, or regenerated).


5. Click on the top.
   A **Certificate History** screen pops up with details corresponding to the selected certificate.

## Add an Application Connector to a Server Certificate Topology

To add an application connector to a server certificate topology:

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.
5. On the Certificate topology page, click .
6. On the **Add Connector** pop-up window, select the device type from the **Category** dropdown.
7. Select the device vendor from the **Vendor** dropdown.
8. In the **Connector Name** field, enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
9. Enter a description for the connector.
   This description shows up when you hover over the connector within the Certificate topology.

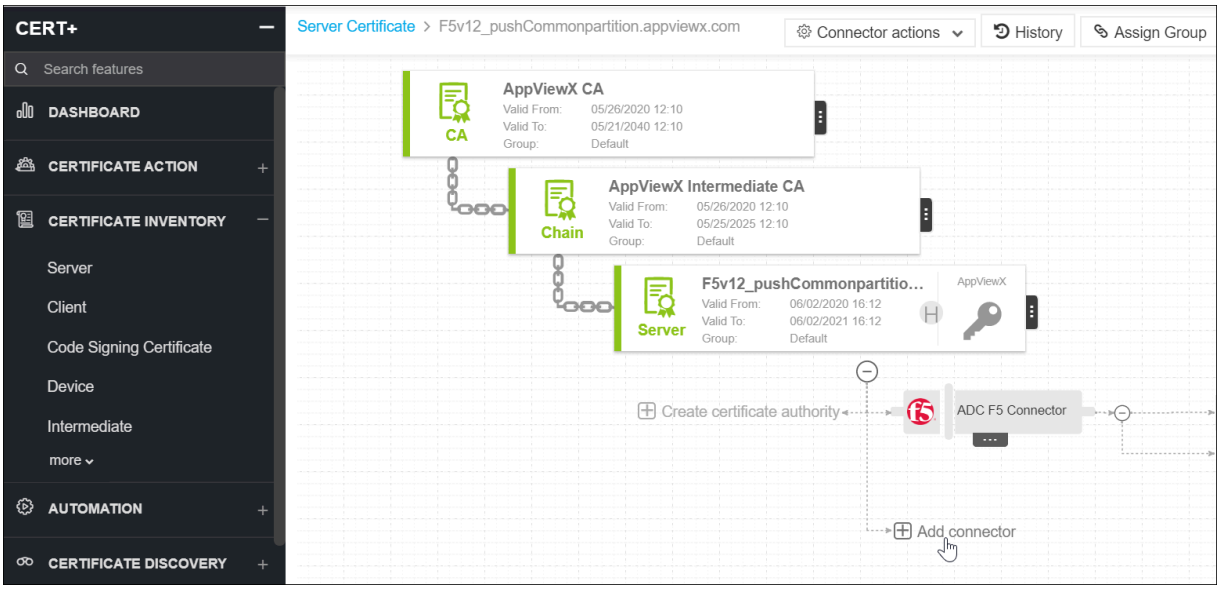
   **Note:** Only applicable for **Citrix** application type

   The SNI-enabled virtual server option will be displayed. When this checkbox is selected, the virtual servers whose SNI are enabled will be listed. Also, you can enable SNI for the virtual server by selecting **Enable SNI push for Certificate** and **Enable SNI in Virtual Server**
10. From the list of available application objects, click » beside each device you want to select.
11. From the Certificate type dropdown, click the type of certificate to be used with the connector.
12. From the Certificate file name field, enter the name of the certificate.
    The file format of the selected certificate type will be automatically displayed.
13. In the **Key File Name** field, enter a name for the key file.

14. Select the **Push root and intermediate certificates** to be pushed to the device.
15. In the Script location field, specify whether the **Pre - Push script** and **Post - Push script file** is In AppViewX or device.
16. Enter the script location that must be executed before and after the push in the **Pre - Push script** and **Post - Push script** fields respectively.
17. Select the **Overwrite** checkbox to overwrite existing certificates with the new certificate.
18. Select Push automatically checkbox to push certificates to the device automatically.
    (Only applicable for **F5** application type) The **Secure Push** checkbox will be selected by default. This option encrypts certificates while pushing them to a device. You can uncheck this option if you have the necessary permissions.

> **Note:** For .jks Keystore, a valid alias has to be entered to reference the certificate within the key store.

19. Click **Save** to add the application connector to the Certificate topology.




## Add an Application Connector to a Client Certificate Topology

To add an application connector to a client certificate topology:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Client**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the Certificates list view, click the **Common Name** of a certificate you want to add a connector to.

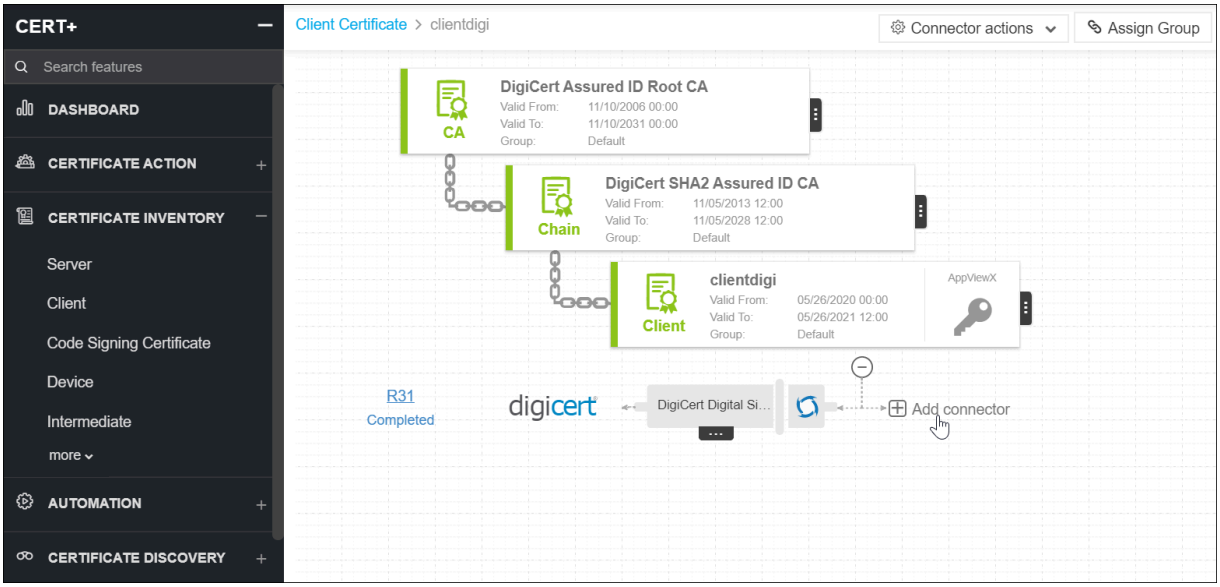
5. On the Certificate topology page, click +.
6. On the **Add Connector** pop-up window, select the device type from the **Category** dropdown.
7. Select the device vendor from the **Vendor** dropdown.
8. In the **Connector Name** field, enter a name for the connector that is descriptive enough when viewed within the Certificate topology.
9. Enter a description for the connector.
   This description shows up when you hover over the connector within the Certificate topology.

   **Note:** Only applicable for **Citrix** application type

   The SNI-enabled virtual server option will be displayed. When this checkbox is selected, the virtual servers whose SNI are enabled will be listed. Also, you can enable SNI for the virtual server by selecting **Enable SNI push for Certificate** and **Enable SNI in Virtual Server**
10. From the list of available application objects, click » beside each device you want to select.
11. From the Certificate type dropdown, click the type of certificate to be used with the connector.
12. From the Certificate file name field, enter the name of the certificate.
    The file format of the selected certificate type will be automatically displayed.
13. In the **Key File Name** field, enter a name for the key file.
14. Select the **Push root and intermediate certificates** to be pushed to the device.
15. In the Script location field, specify whether the script file is In AppViewX or device.
16. Enter the following script and parameter details. Note that only the Push script location field is required:
    - Pre-Push script location and Pre-Push script parameters
    - Push script location and Push script parameters
    - Post-Push script location and Post-Push script parameters
    - Monitor script location and Monitor script parameters
    - Rollback script location and Rollback parameters
17. Select the **Overwrite** checkbox to overwrite existing certificates with the new certificate.
18. Select Push automatically checkbox to push certificates to the device automatically.
    (Only applicable for **F5** application type) The **Secure push** checkbox will be selected by default. This option encrypts the certificates while pushing them to a device. You can uncheck this option if you have the necessary permissions.

    **Note:** For .jks Keystore, a valid alias has to be entered to reference the certificate within the key store.

19. Click **Save** to add the application connector to the Certificate topology.

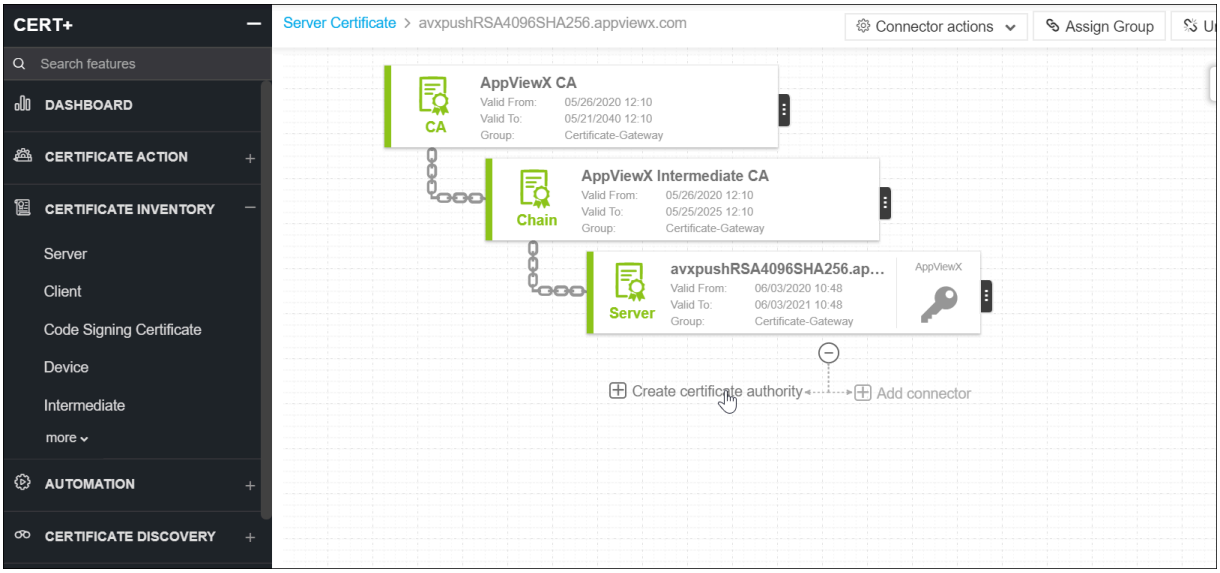



## Add a Certificate Authority Connector to a Certificate Topology

To add a Certificate Authority (CA) connector to a server or client certificate topology:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device,** or **Code Signing** depending on the type of certificate you want to add a CA connector to.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the Certificates list view, click the **Common Name** of a certificate you want to add a Certificate Authority Connector to.
5. On the Certificate topology page, click **Create Certificate Authority**.
6. On the details page, in the **Assign Group** field, select a group to assign the certificate.
7. In the **Certificate Authority** field, select a CA from the dropdown. Other fields on the page change depending on the selected certificate authority. For each type of certificate authority, fields marked with a * are mandatory.

8. Click **Add**.




## Enroll a Certificate

To enroll a certificate:

1. Click ☰ and select **CERT+** > **Certificate Action**.
2. Under **Certificate Action**, click **Enroll Certificate** and select **Server**, **Client**, or **Code Signing** depending on the type of certificate(s) you want to enroll.
3. On the **Enroll Server Certificate** details page, under **General Information**, assign a group to the certificate.
4. Under **CA Details**, in the **Certificate Authority** field, select a CA for the certificate. Other fields and options vary depending on the CA you chose.
5. Choose a **CSR Generation** mode: AppViewX, Upload CSR, HSM, or Endpoint. For all the CA types except Amazon, you have the option to generate the CSR. Fields displayed will vary for each CSR generation method.

> **Note:** For Microsoft Enterprise, Microsoft Standalone, and Entrust CA(s), provide the **Subject Alternative Name** for certificates by selecting Directory Name, DNS, Email, IP Address, Registered ID, URL, and Other Names.

6. Under **CSR Parameters**, enter a **Common Name** for the certificate and fill in all the mandatory fields.
7. While creating certificates, the user can attach supporting documents by uploading it in the **Attachment** section.

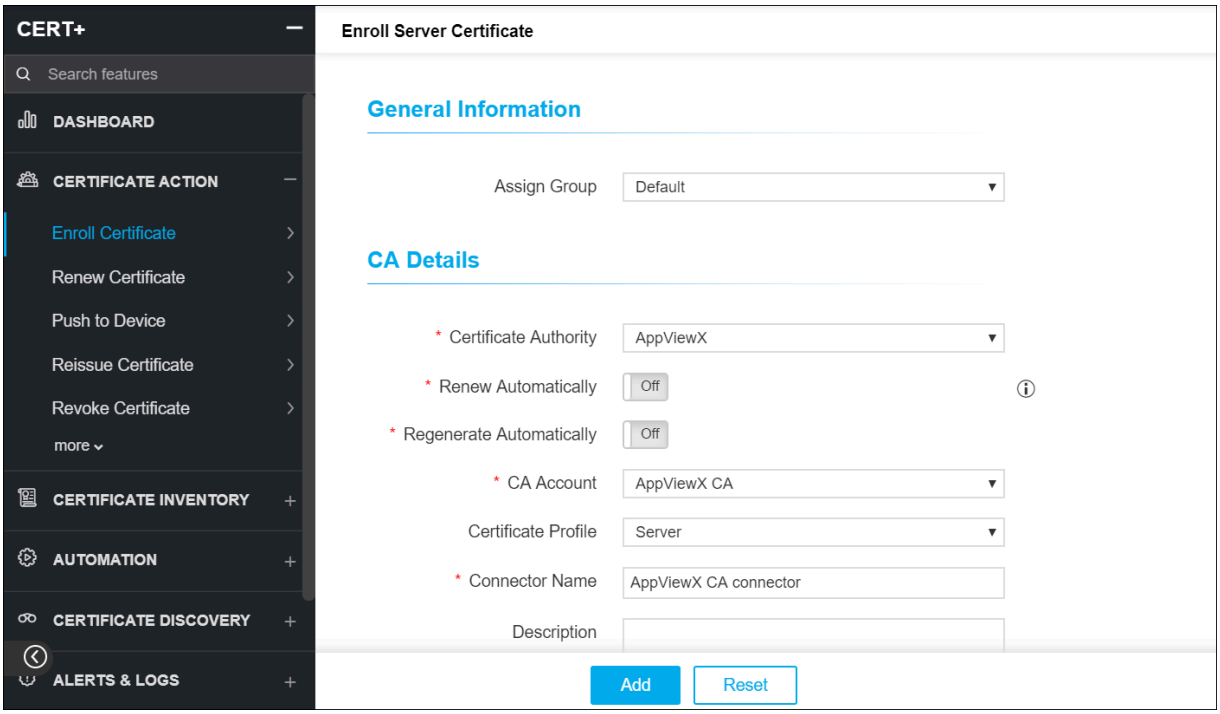
8. Click **Add** to generate the certificate.
   The certificate holistic view with the newly created CSR appears.
9. Click **Submit**.
10. On the **Submit** pop up window, enter relevant comments and click **Yes**.
    A request ID and work order ID are generated automatically and the work order status In Progress (Approval level 1) is displayed beside the connector on the topological view.
11. Click **Approve** to approve the work order.
12. On the Approve pop up window:
    - Turn **On** or **Off** the **Manual Implementation**.
    - Select the **Implementation Time**.
    - Enter comments to approve the CSR and click Yes.

    The work order status displayed beside the connector updates to In Progress (CSR submission).
13. Click **Implement** to submit the request to the CA.
14. On the **Implement** pop up window:
    - Turn **On** or **Off** the **Manual Implementation**.
    - Select the **Implementation Time**.
    - Enter comments to implement the request and click **OK**.

    The work order status displayed beside the connector updates to **In Progress (Awaiting certificate retrieval)**.
15. Click (Refresh) on the top to update the topology. After the CA is generated, the status updates to **Completed**.

> **Note:** You can perform a wide range of actions on the certificate by hovering over  and selecting one of the options in the dropdown.

16. To return to the certificate list view and view the new certificate, click Certificate on the top left.
17. After CSR is requested, to view details in the certificate holistic page, hover over the **CA Connector** icon and click **View**.




**Note:** You can enable **Automatic CSR Generation** during the certificate enrolment process in CERT+.

## Enroll a Code Signing Certificate

A code signing certificate contains a digital signature to verify the author's identity and to ensures that the code (executable/script) is not modified after the author's signatory.

To enroll a code signing certificate:

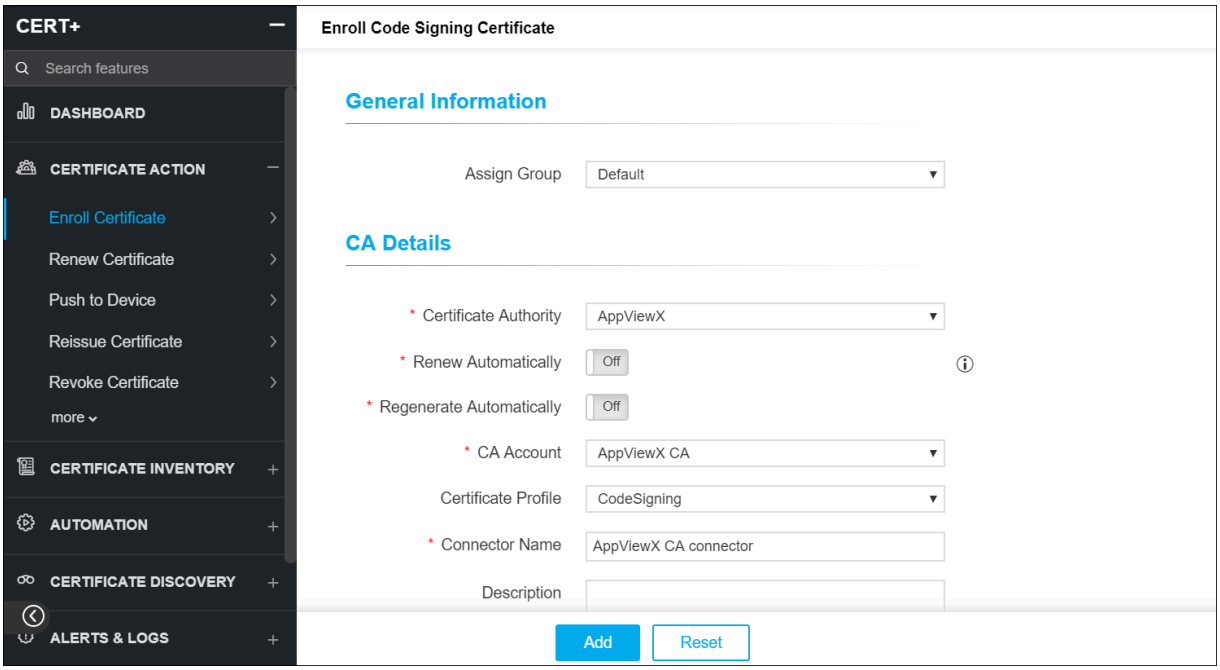
1. Click and select **CERT+** > **Certificate Action**.
2. Under **Certificate Action**, click **Enroll Certificate>> Code Signing Certificate**.
3. On the **Enroll Code Signing Certificate** page, under the **General Information** section, assign a group to the certificate.
4. Under the **CA Details** section, in the **Certificate Authority** field, select the CA for the certificate.

**Note:** Other fields in the **CA Details** section vary depending on the CA you choose. * denotes mandatory fields.

5. Under the **CSR Parameters** section, enter the following mandatory fields:

- Common name - The fully qualified domain name (FQDN) or common name that exactly matches your web browser.
- **Validity (in years)** - The duration for which the certificate must be valid.
- Hash function - Select either SHA256 or SHA160, depending on which hash algorithm you want to use.
- Key type - Select either RSA or DSA depending on the type of security algorithm you want to use.
- Bit length - Choose the length of the key you want to generate: 4096, 2048, 1024, or 512 bits.

6. Click on **Upload** to attach a file.
7. Enter **Certificate Attributes** and **Generic Fields**.
8. Click **Add**.




## Push a Certificate to a Device

The push to device option allows you to push the certificate to the load balancer or server device and associate it to a profile, template, or virtual server. If the Push automatically field is selected while adding application connectors to a new certificate, then the certificate is automatically pushed to the device when it is retrieved. In this case, users need not complete the process manually.

## Prerequisites

Before pushing the certificate to a device, ensure that you have the necessary role-based access controls and workflow access of the template and request.

To push a certificate to a device:

1. On the Certificate list view page, locate the certificate you want to push and click its name on the **Common Name** column.
2. On the certificate topology page, click **Push to Device**.
3. On the **Confirmation** pop up window, enter comments and click **OK**.
   A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.
4. Click **Approve** to approve the push request.
5. On the Confirmation screen that pops up:
   a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
   b. If you select **Off**, set the date and time that you want the cert push to occur.
   c. Enter comments and click **Yes**.
   The work order status displayed beside the connector updates to **Push-Review In Progress**.
6. Click **Implement** to implement the push request.
7. On the Confirmation screen that pops up:
   a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
   b. If you select **Off**, set the date and time that you want the cert implementation to occur.
   c. Enter comments and click **Yes**.
8. Click  on the top of the page until the topology updates.
   After the push action is completed, the status updates to **Completed**. The topological view follows a color-coding scheme to identify certificate status.

| Color | Certificate Status |
|---|---|
| Green | The certificate is available and valid. |
| Red | The certificate has expired. |
| Gray | Certificate push action failed. |
| Blue | The certificate will expire in 90 days. |
| Yellow | The certificate will expire in 30 days. |
| Orange | The certificate will expire in 10 days. |
| Black | The certificate has been revoked. |
| Mid Purple | The certificate associated with profiles is manually removed. |

## Renew a Certificate

## Through Holistic View

To renew a certificate from the holistic view:

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client,** or **Device** depending on the type of certificate you want to renew.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over on the certificate and click **Renew**.
6. On the Renew pop up window, in the **Renew Automatically** field, click Off to change it to On.
7. Enter the number of days before which the certificate renewal must be initiated.
8. Click **Renew**.
9. On the **Renew** pop up window, enter comments and click **Yes**.
   A request ID and work order ID are then generated automatically and the work order status is displayed beside the certificate on the topological view.
10. Click **Approve** to approve the renew request.
11. On the Approve screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert renewal approval to occur.
    c. Enter comments to approve the renewal, then click **Yes**. The work order status is displayed beside the connector.
12. Click **Implement** to implement the renewed request.
13. On the screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert renewal implementation to occur.
    c. Enter comments to approve the renewal, then click **Yes**.
14. Click icon on the top-right until the topology updates.
    After the renew action is completed, the status updates to **Completed**.

## Through Command bar

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client,** or **Device** depending on the type of certificate you want to renew.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificates list view, select a certificate you want to renew.

5. Click **Actions** and select **Renew Certificate**.
   The **Renew Certificate** window appears.
6. Depending on when you want to renew the certificate(s), select one of the following options:
   - **Now** - The certificate(s) is renewed immediately.
   - **Set auto-renew** - The certificate(s) can be configured for an automatic renewal ranging between 1 to 90 days.
7. Click **Submit**.

## Regenerate a Certificate

The regenerate option allows you to create a new certificate with similar parameters of an existing certificate that you can host it on a different type of web or application.

To regenerate a server certificate:

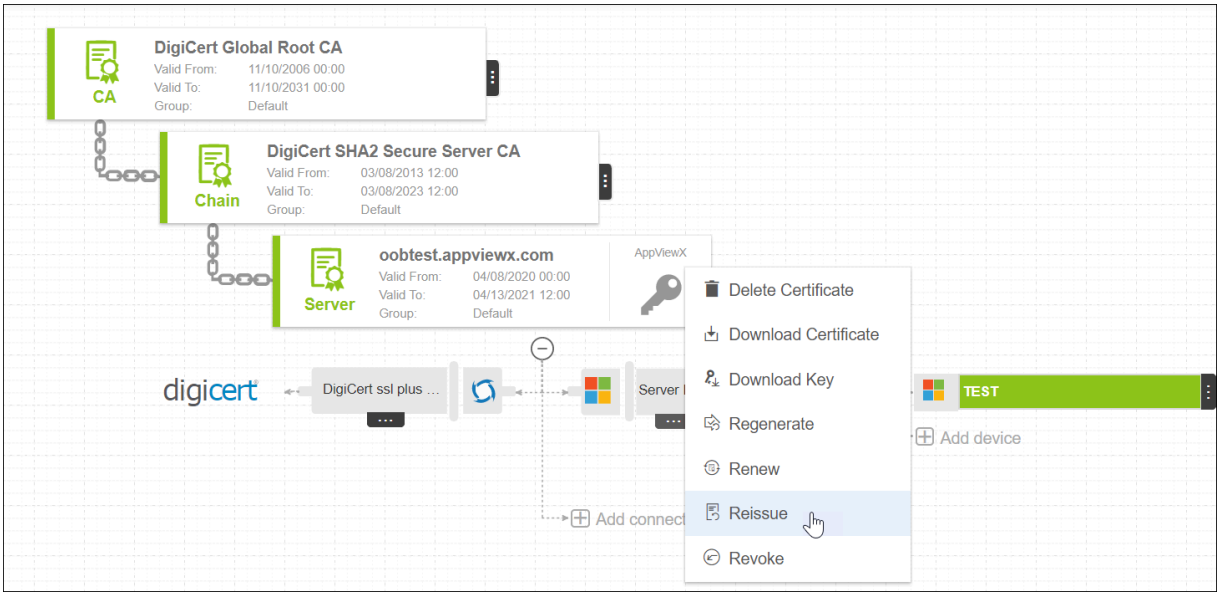
1. Click  and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over  on the certificate and click **Regenerate**.
6. On the Regenerate page, make changes if required and click **Regenerate**. The certificate is regenerated and the topology screen opens.
7. Click **Approve**.
8. On the Approve screen that pops up:
   a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
   b. If you select **Off**, set the date and time that you want the cert regeneration approval to occur.
   c. Enter comments to approve the regeneration, then click **Yes**.
9. Click the **Implement** button that appears.
10. On the Implementation screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert regeneration implementation to occur.
    c. Enter comments to implement the regeneration and click **Yes**.
    A request ID and work order ID are generated automatically and the work order status is displayed beside the certificate on the topological view.
11. Click  on the holistic view to refresh the screen.
    The work order status is displayed beside the certificate.

12. Click  on the Command bar until the topology updates.
    After the regenerate action is completed, the status updates to **Completed**.

## Reissue a Certificate

To reissue a server certificate:

1. Click  and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client,** or **Device** depending on the type of certificate you want to reissue.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over  on the certificate and click **Reissue**.




   Depending on the type of certificate you are reissuing, the Reissue screen appears.
6. Click **Reissue**.
7. On the Reissue pop up window, enter the reason and comments and click **Yes**.
   A request ID and work order ID are generated automatically and the work order status is displayed beside the certificate on the topological view.
8. Click **Approve** to approve the reissue request.
9. On the Approve screen that pops up:

a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
b. If you select **Off**, set the date and time that you want the cert reissue approval to occur.
c. Enter comments to approve the reissue, then click **Yes**.

The work order status is displayed beside the connector.

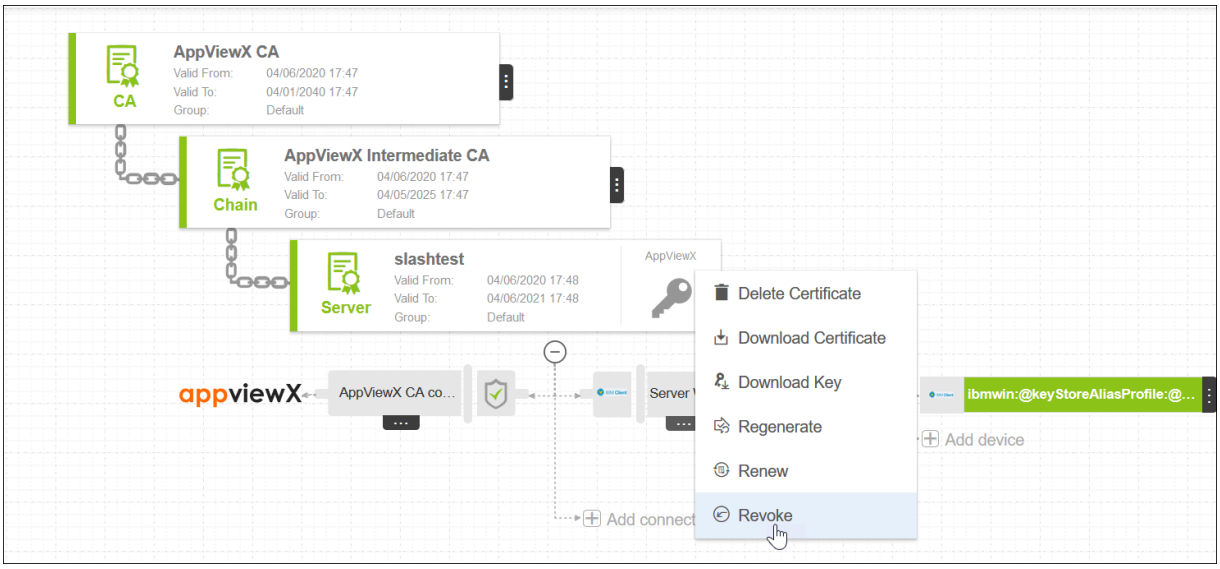
10. Click  on the holistic view to refresh the screen.
    The work order status is displayed beside the certificate.
11. Click **Implement** to implement the reissued request.
12. On the screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the cert reissue implementation to occur.
    c. Enter comments to approve the reissue, then click **Yes**.
13. Click  on the top-right until the topology updates.
    After the reissue action is completed, the status updates to **Completed**.

## Revoke a Certificate

If you have the necessary permission, you can submit a request to the certificate authority to revoke it. As soon as the certificate is revoked, the certificate is no longer considered to be trusted. Revoked certificates are listed in the Certificate Revocation List (CRL) maintained by each certificate authority.

To revoke a certificate:

1. Click  and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client,** or **Device** depending on the type of certificate you want to revoke.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over  on the certificate and click **Revoke**.




6. On the **Certificate Revoke** pop up window, select a reason for revoking the certificate.
7. In the **Comments** field, enter details for revoking the certificate.
8. Click **Yes**.

   A request ID and work order ID will be generated automatically and the work order status will be displayed beside the certificate on the topological view.
9. Click **Approve** to approve the revoke request.
10. On the **Approve** screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time you want the certificate revocation approval to occur.
    c. Enter **comments** to approve the revocation, then click **Yes**.

    The work order status will be displayed beside the connector.
11. Click the **Refresh** icon on the top until the topology updates.
12. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
13. Click **Implement** to implement the revocation request.
14. On the screen that pops up:
    a. If you select **Off**, set the date and time that you want the certificate renewal implementation to occur.
    b. Enter **comments** to approve the revocation, then click **Yes**.

    The work order status will be displayed beside the connector.
15. Click  on the top until the topology updates.

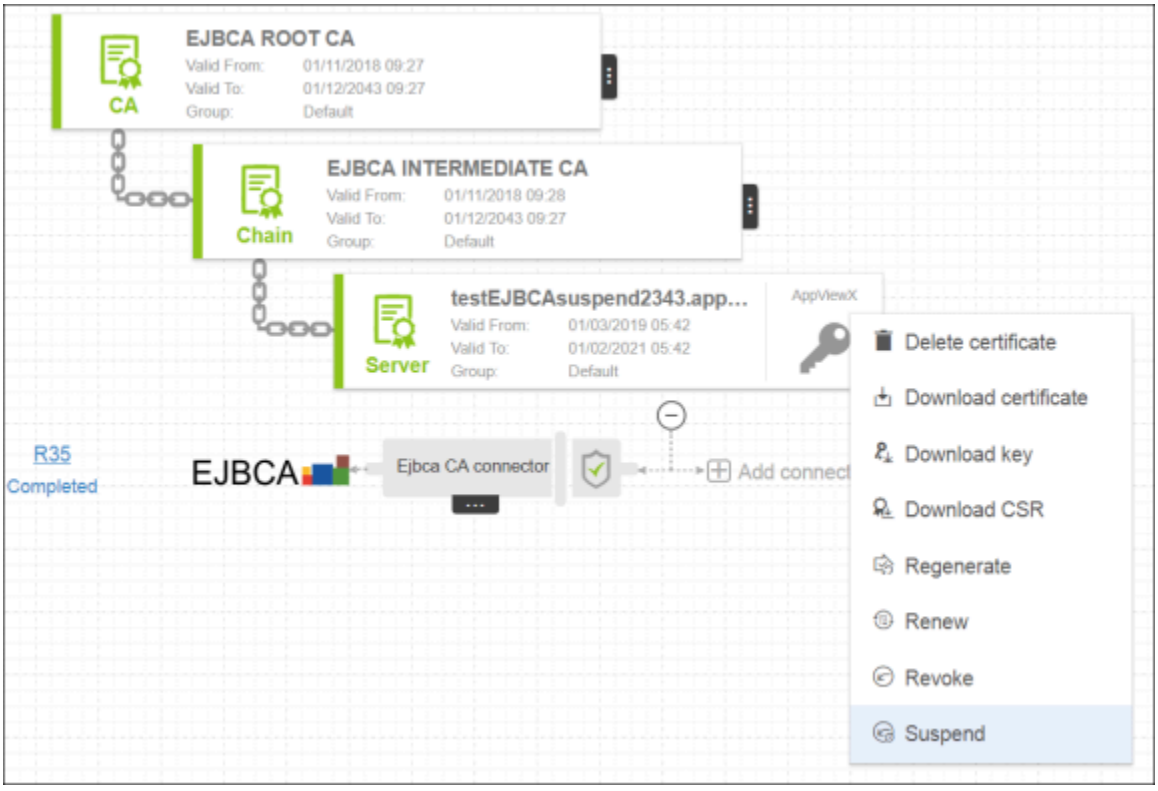
    After the revoke action is completed, the status updates to **Completed**.

## Suspend Certificate

If you have the necessary permission, you can suspend a certificate. As soon as the certificate is suspended, it is revoked. The suspended certificates are listed on the Certificate Revocation List (CRL) maintained by each certificate authority.

To suspend a certificate:

1. Click ☰ and select **CERT+**.
   The **CERT+** left navigation pane appears.
2. Switch to the **List** toggle button on the top right corner of the page.
3. Click **Server, Client,** or **Device** tab depending on the type of certificate you want to suspend.
4. In the **Common Name** column certificate list, select the certificate that you want to suspend.
   The certificate topology appears on the screen.
5. Hover the mouse over ⋮ on the certificate, and click the **Suspend** option.




6. In the **Comments** field, enter the reason for suspending the certificate.
7. Click **Yes.**

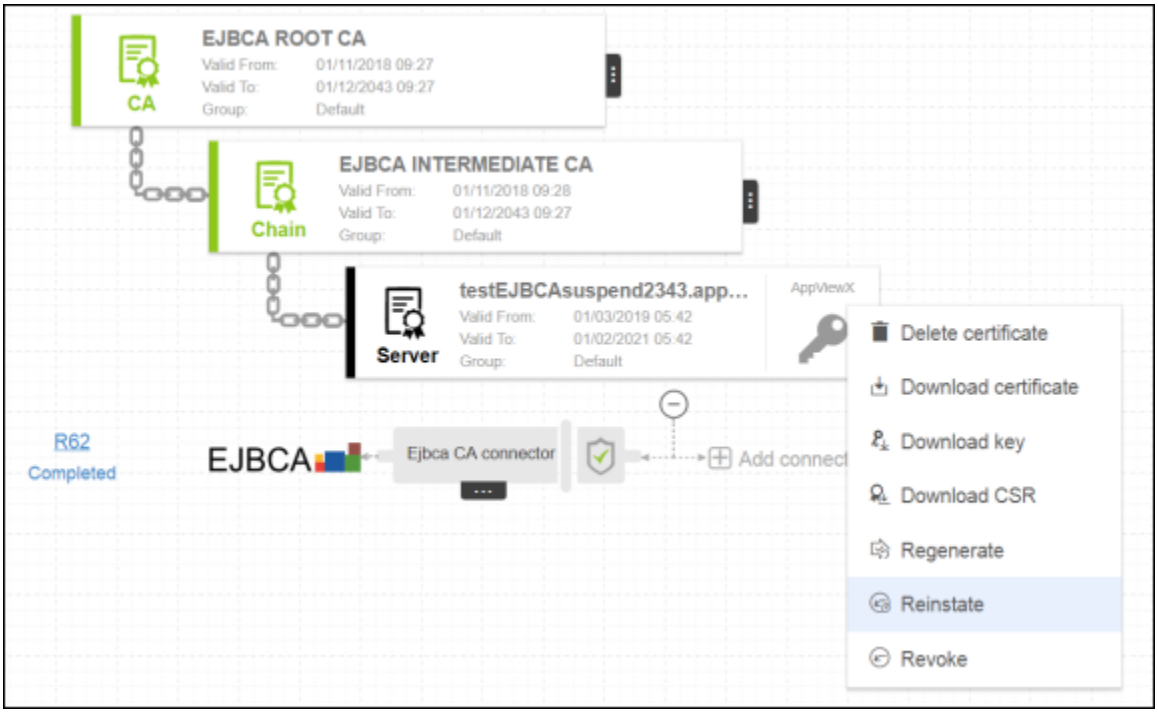
## Reinstate a Certificate

You can reinstate a suspended certificate if you have the necessary permissions.

**Note:** This option is available only for **Microsoft** and **EJBCA** certificate authorities.

To reinstate a certificate:

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over on the certificate and click **Reinstate**.



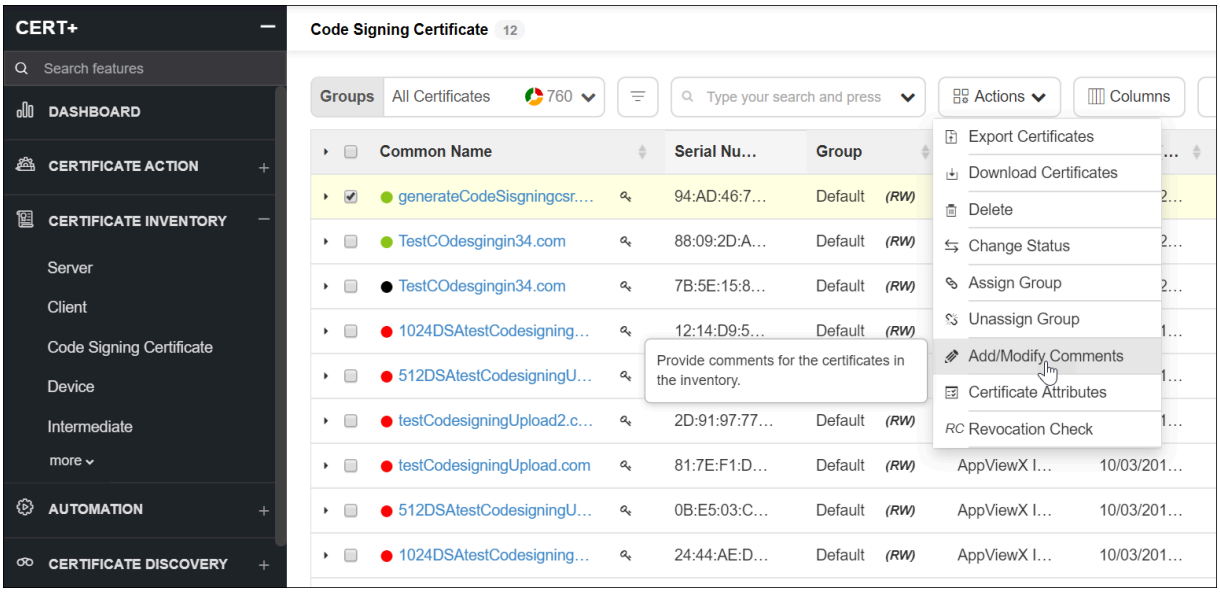

6. On the Certificate reinstate pop up window, select a reason for reinstating the certificate.
7. In the **Comments** field, enter details for reinstating the certificate.
8. Click **Yes**.

## Add/Modify Comments

To add/modify comments for certificate(s):

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**,**Device ,**or**Code Signing**tab depending on the type of certificate(s) you want to add/modify comments.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) for which you want to add/modify comments.
5. Click **Actions** and select **Add/Modify Comments** option from the dropdown.
6. On the **Add/Modify Comments** pop-up window, add a new comment or modify the existing comment.
7. Click **Save**.

   The new/modified comment for the selected certificate is displayed on the **Comments** column.




## Perform Revocation Check

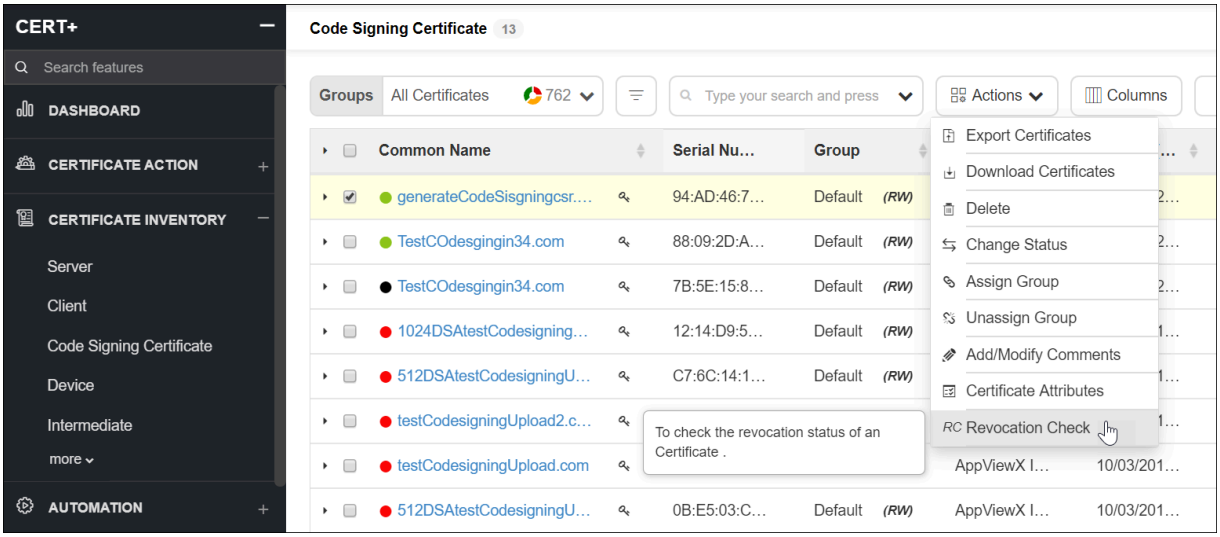
For CAs (both external and AppViewX), you can check the most recent status of the certificate even if it is moved to the inventory for the first time. This check is performed automatically twice a day and the user can check for the revoked certificates anytime.

To perform a revocation check:

1. Click ☰ and select **CERT+**.

   The **CERT+** left navigation pane appears.
2. Click **Server**, **Client**, **Device** or **Code Signing** depending on the type of revoked certificates you want to view.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) for which you want to check the revocation.

5. Click **Actions** and select **Revocation Check** option from the dropdown.
6. On the **Revocation Check** pop up window, click **OK**.
   The status of the revoked certificate is displayed on the **Valid for** column.




## Roll Back a Certificate from a Device

The Rollback option allows you to revert to the previous successful certificate pushed to an SSL profile or template. Rolling back to the last known good state can be performed only from the individual profile level and the Rollback option only appears in the dropdown **Action** list if a certificate has already been successfully pushed to the device.

## Prerequisites

Before rolling back a certificate that was pushed to a device, ensure that you have the necessary role-based access controls and workflow access to the template and request.

To roll back a certificate from a device,

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Click **Rollback**.
6. On the Confirmation screen that pops up, enter comments to rollback a certificate, then click **OK**.
   A request ID and work order ID are generated automatically and the work order status is displayed beside the connector on the topological view.

7. Click **Approve** to approve the rollback request.
8. On the Approve screen that pops up:
   a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
   b. If you select **Off**, set the date and time that you want the certificate rollback to occur.
   c. Enter comments to approve the rollback, then click **Yes**. The work order status is displayed beside the connector.
9. Click **Implement** to implement the rollback request.
10. On the screen that pops up:
    a. Click **On** or **Off** button in the **Manual Implementation** field to choose the mode of implementation.
    b. If you select **Off**, set the date and time that you want the certificate rollback implementation to occur.
    c. Enter comments to approve the rollback, then click **Yes**.

    The work order status is displayed beside the connector.
11. Click  on the top-right until the topology updates.

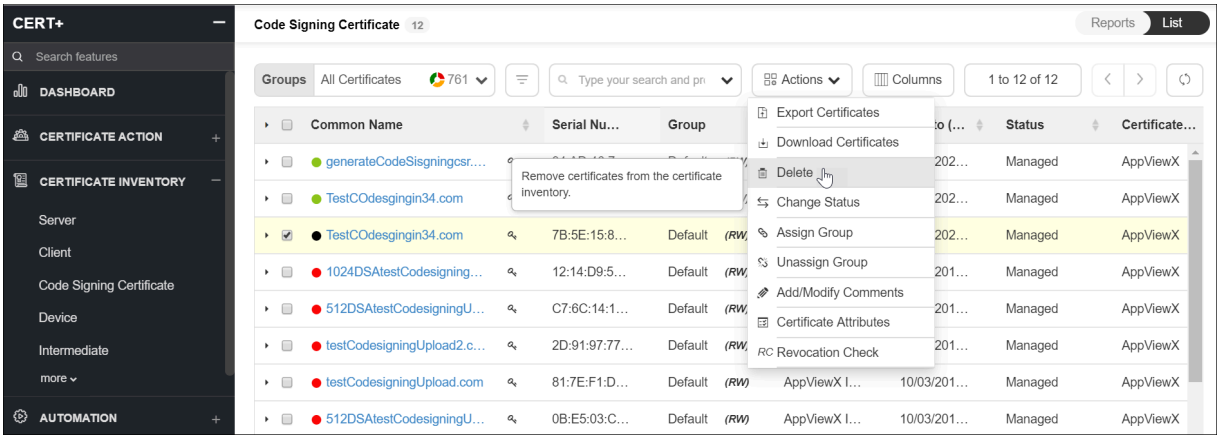
    After the rollback is completed, the status updates to **Completed** and the color of the connector changes to gray.

## Delete a Certificate

To delete a certificate:

1. Click  and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to delete.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) you want to delete.
5. Click **Actions** and select the **Delete** option from the dropdown.
6. On the Delete Certificate pop-up window, click **Yes**.

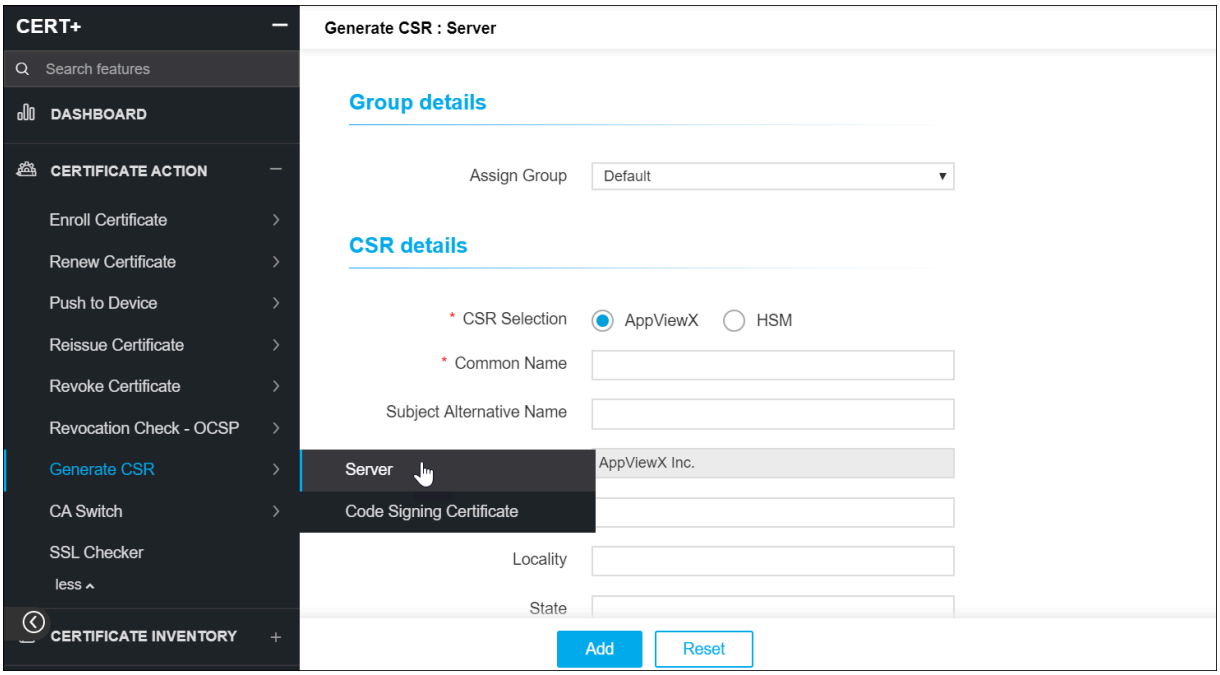
The certificate is then removed from the list and deleted from the AppViewX system.




## Generate a CSR for a Certificate

To generate a certificate signing request (CSR) for a certificate:

1. Click ☰ and select **CERT+** > **Certificate Action**.
2. Under **Certificate Action**, click **Generate CSR** and select **Server** or **Code Signing** certificate.
3. On the Generate CSR page, enter the details under **Group Details** and **CSR Details** section. Fields on the screen vary depending on the type of certificate you are generating a CSR for. Fields marked with a * are mandatory.
4. Click **Add** to generate the CSR and add it to the group.



## Submit a CSR to a Certificate Authority

After you have generated a CSR, you must submit it to the respective certificate authority (CA) for signing. To do this:

1. Add a **CA Connector** to the certificate topology.
2. On the Certificate list view, locate the CSR you generated and click its name on the **Common Name** column. The certificate topology screen opens.
3. Click **Submit** and on the Submit pop up window, enter comments and click **Yes**.
4. A request ID and work order ID are generated automatically and the work order status is displayed beside the server certificate node as In Progress (Approval level 1).
5. Click **Approve** and on the Approve pop up window, click **Yes**.
6. The work order status displayed beside the server certificate node changes to **In Progress** (Awaiting implementation).

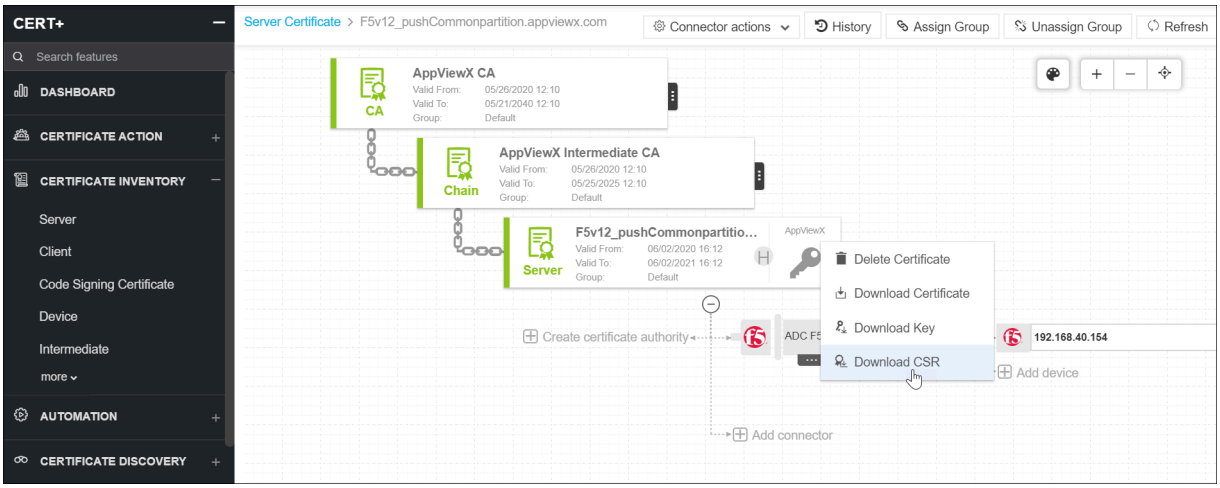
> **Note:** If the Approval required checkbox was not selected when the policy was created. After submitting the request, the Approval and Implementation process is skipped and the workflow jumps directly to the **Awaiting Certificate Retrieval** process.

7. Click **Implement** and on the screen that pops up:
   - Click ON if you want to manually implement the CSR request.
   - Click OFF if you want to set auto-implementation. If you select this option, set the date and time that you want the implementation to occur.
8. Click **OK** to close the popup screen.
   The work order status updates to **In Progress** (CSR Submission). The CSR request is then submitted to the appropriate CA for verification so that an SSL certificate can be generated and retrieved by AppViewX. Depending on the CA, this process might take some time, in which the work order displays a status of Awaiting Certificate Retrieval.
9. Click  on the command bar until the topology updates.
   When the generated certificate is successfully retrieved, a Chain of Trust displays on the topology and the status updates to **Completed**.

## Download a CSR for a Certificate

To download a certificate signing request (CSR) for a certificate:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over ⋮ on the certificate and click **Download CSR**.




## Assign or Unassign a Group to a Certificate

## Assign a Group

To assign a group to a certificate:

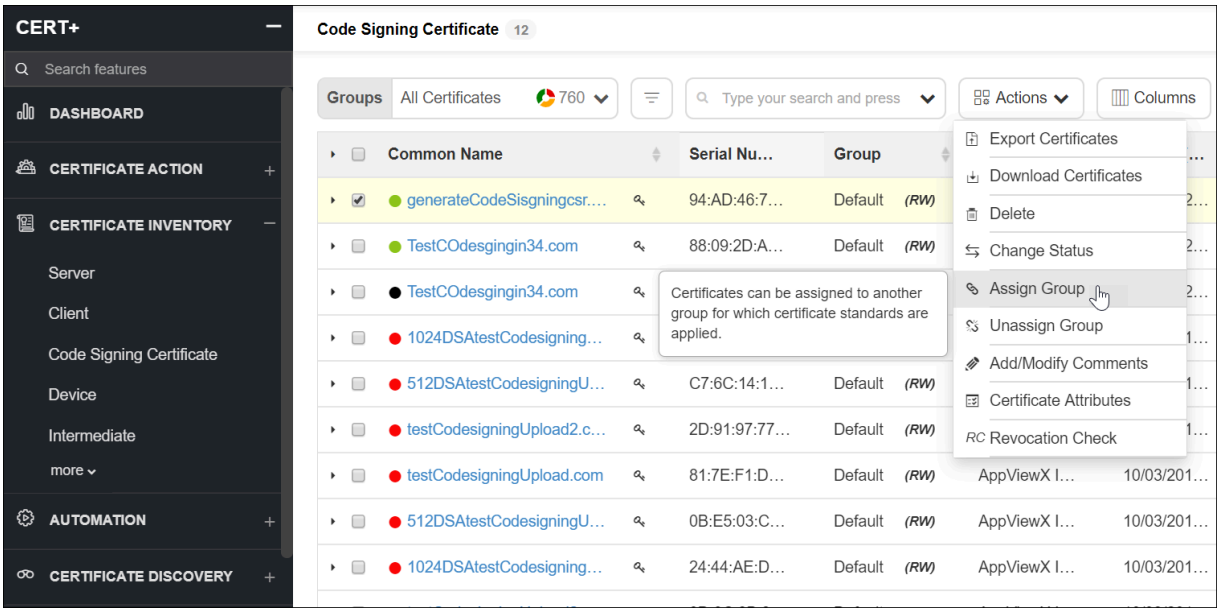
1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to assign a group to.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) for which you want to assign a group.
5. Click **Actions** and select the **Assign Group** option from the dropdown.
6. On the **Assign to Group** pop-up window, select a group.
7. Click **Assign**.

## Unassign a Group

To unassign a group from a certificate:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to assign a group to.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) you want to unassign from a group.
5. Click **Actions** and select the **Unassign Group** option from the dropdown.
   It automatically unassigns the group.

> **Note:** You cannot unassign a certificate from the **Default** group. If you unassign a certificate from the assigned group, it will be assigned to the **Default** group.




## Change the Status of a Certificate

Before changing the status of a certificate, the user should plan for the impact that might have on existing work orders.

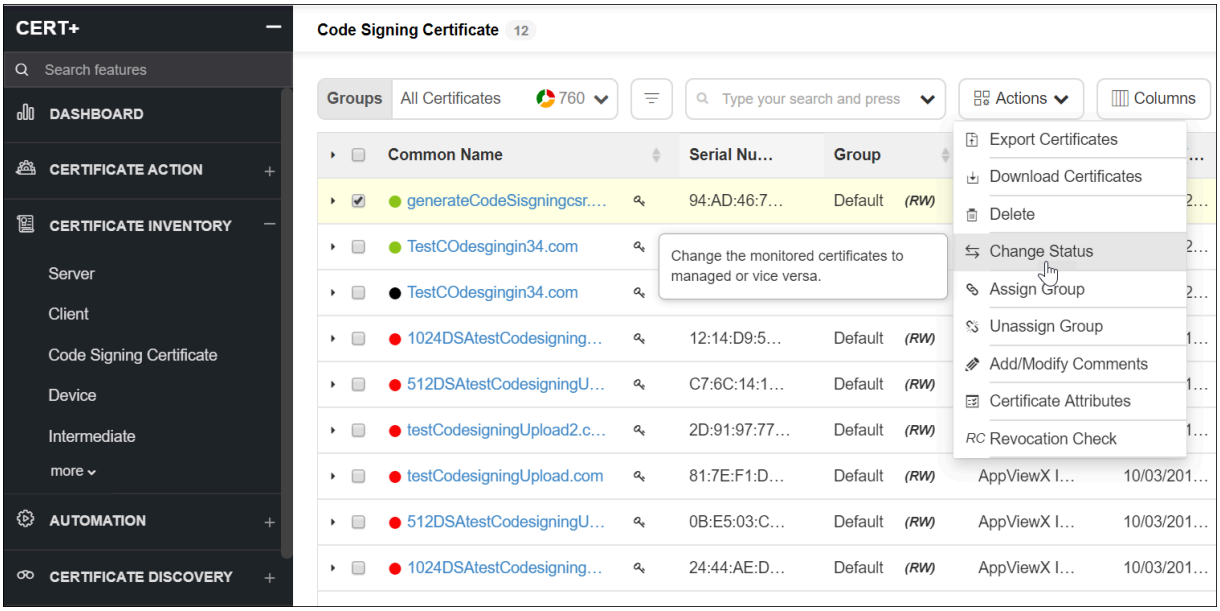
To change the status of a certificate:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to change the status for.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) for which you want to change the status.

5. Click **Actions** and select the **Change Status** option from the dropdown.
6. On the **Change Status**pop-up window, select **Managed**.

> **Note:** (You can perform any actions (Create, Renew, Revoke) on those certificates.) or **Monitored** (For alerting purposes, you will not be able to perform any actions on the certificates) from the **Change Status to** dropdown.

7. In the **Comments** field, enter the reason for changing the status.
8. Click **Yes**.

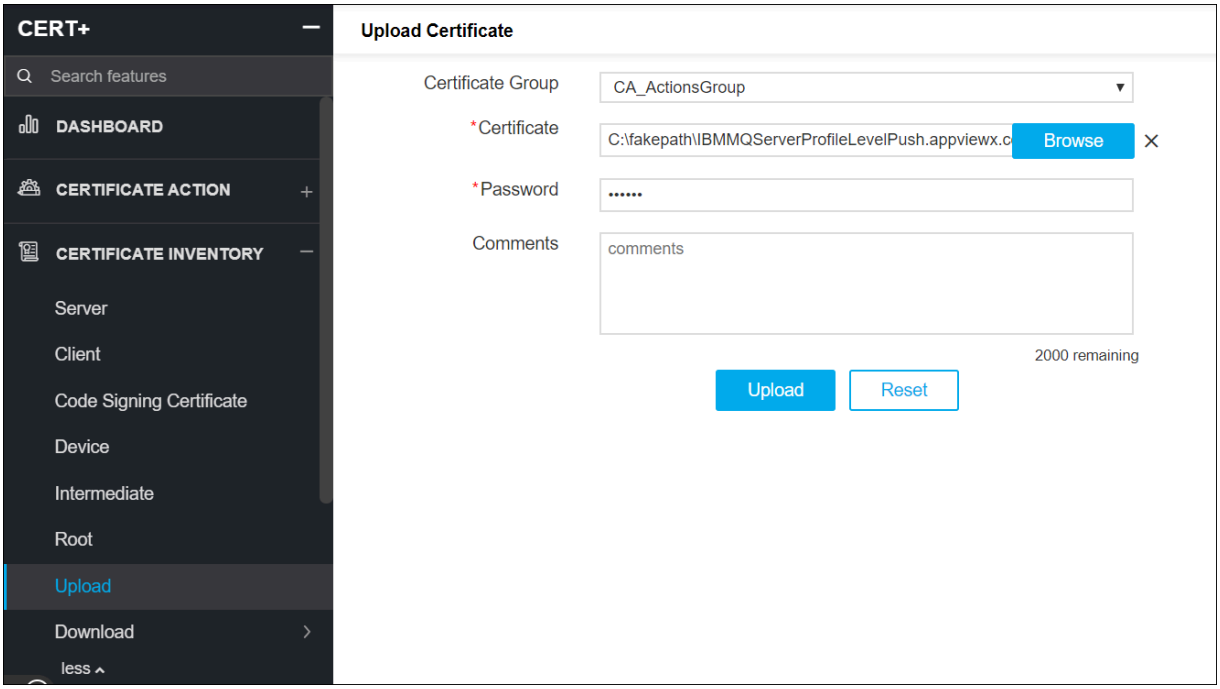



## Upload a Certificate

To upload a certificate:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Upload**.
3. On the Upload Certificate details page, select a **Certificate Group**.
4. Browse and choose the certificate file.
5. Enter relevant comments for uploading the certificate.

6. Click **Upload**.




## Download a Certificate

**Note:** This functionality is available only for server, client, device, intermediate, and root certificates.

You can download a certificate from the Certificate page and the topology page within AppViewX.

## Download from the Certificate Page

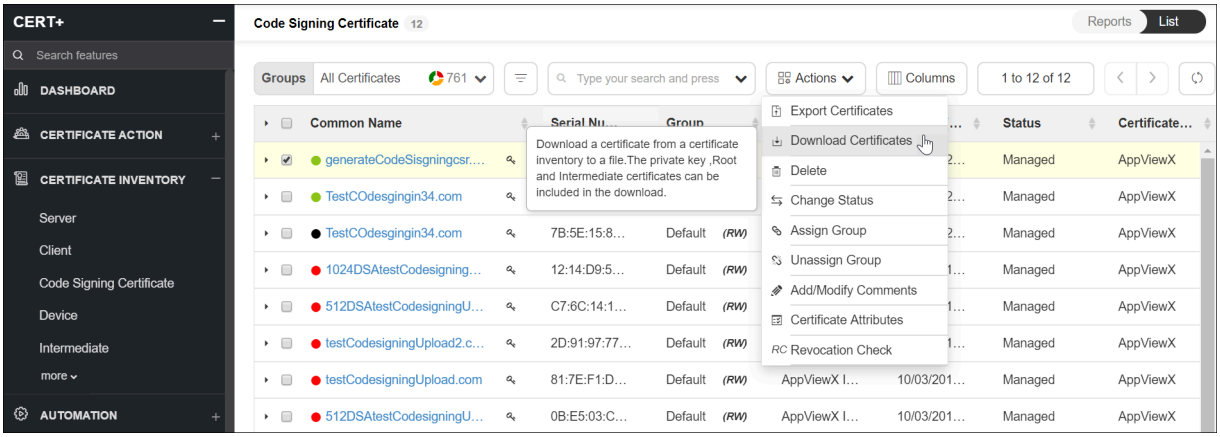
To download a certificate as a **.PEM** file, that is designed to be safe for inclusion in ASCII or rich-text documents such as emails:

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to download.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) you want to download.
5. Click **Actions** and select the **Download Certificates** option from the dropdown.
6. On the **Download Certificate** pop up window, select **Certificates Only** or **Certificates and Keys**.

**Note:** You can also enable/disable **D ownload Truststore Certificates** option along with the end certificates.

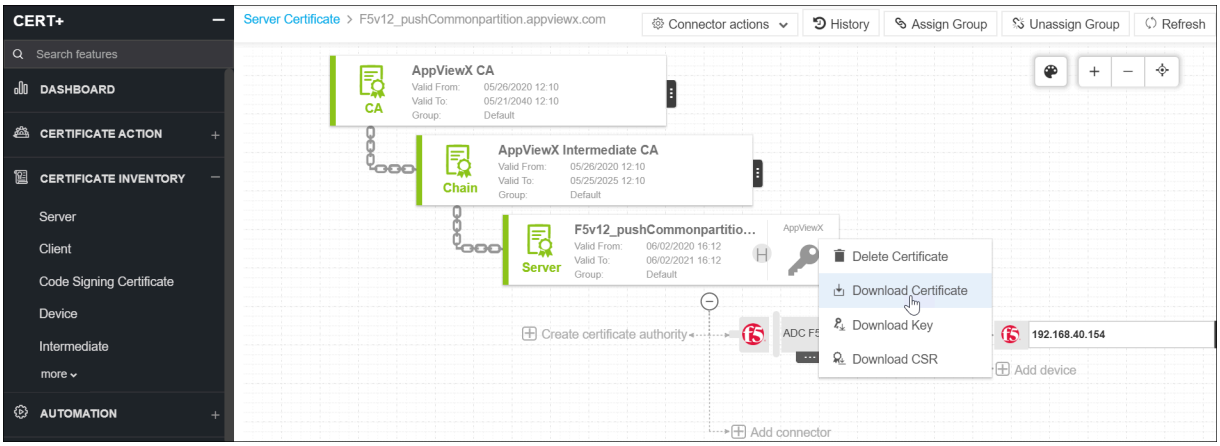
**Note:** If you have permission to view the restricted content mentioned in Step 6, the certificate details are then downloaded inside a zip file. If you do not have the necessary permissions, the system creates and downloads an empty zip file to the destination you specify.

7. On selecting **Certificates and Keys** option**,** the **Secret Passphrase** field appears. Enter a passphrase to encrypt the contents into a ZIP file.
8. Click **Download**.
9. To view details of the certificate, unzip the file and open the security certificate file. Click **Details**.




## Download from the Certificate Topology

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**, **Client**, **Device ,** or **Code Signing** tab depending on the type of certificate you want to download.
3. On the certificate list view, click the **Common Name** of the certificate to view the topology.
4. Hover over ⋮ on the certificate and click **Download Certificate**.




5. On the Download Certificate pop up window, select the file format.

> **Note:** For PEM and DER certificate types, you can enable/disable **Download Truststore Certificates** option along with end certificates.

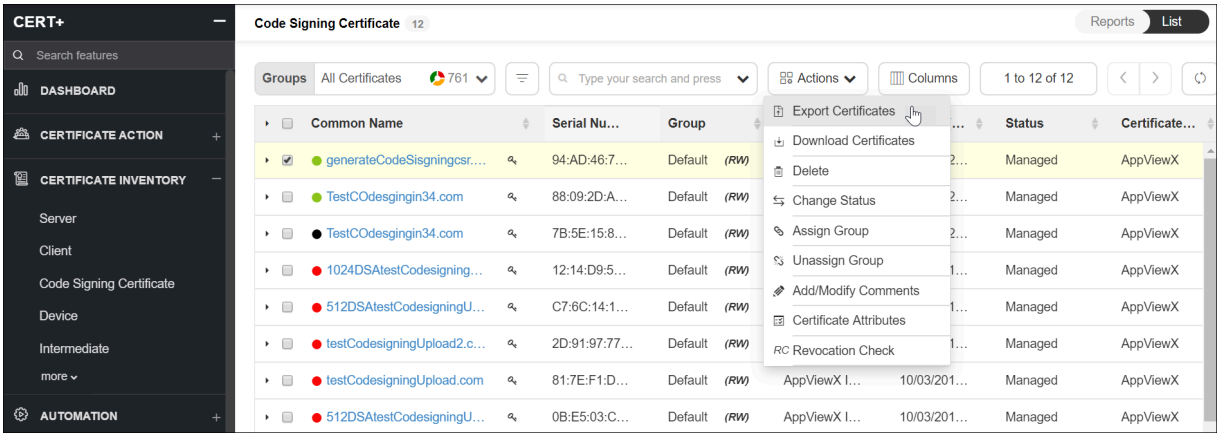
6. Click **Yes**.

## Export Inventory Data of a Certificate

To export inventory data of a certificate:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under Certificate Inventory, click **Server**, **Client**, **Device**, or **Code Signing** tab depending on the type of certificate you want to export.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, select the certificate(s) you want to export.
5. Click **Actions** and select the **Export Certificates** option from the dropdown.
6. On the **Export** pop up window**,** choose whether to export **All Columns** of data for the certificate or **Displayed Columns**.
7. Choose the format **CSV** or **XLS** to save the exported certificate.

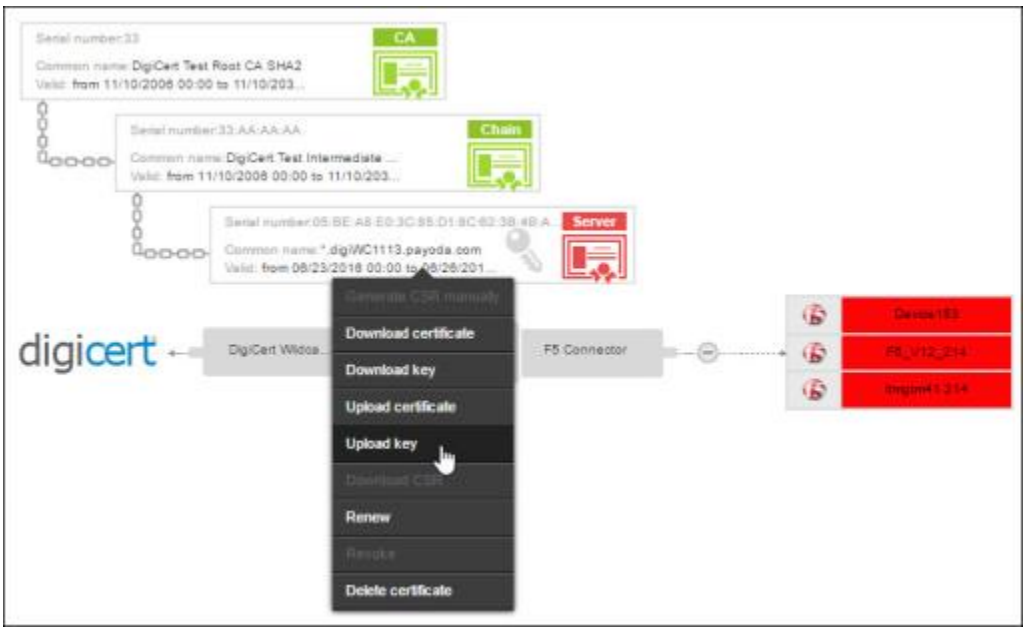
8. Click **Export**.




## Upload a Certificate Key

To upload a certificate key:

1. Click ☰ and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server** or **Clien t**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate for which you want to upload a certificate key.
5. On the certificate topology page, hover over ⋮ on the certificate and click **Upload Key**.



> **Note:** If the key is password-protected, a popup window will appear prompting you to enter the associated password.

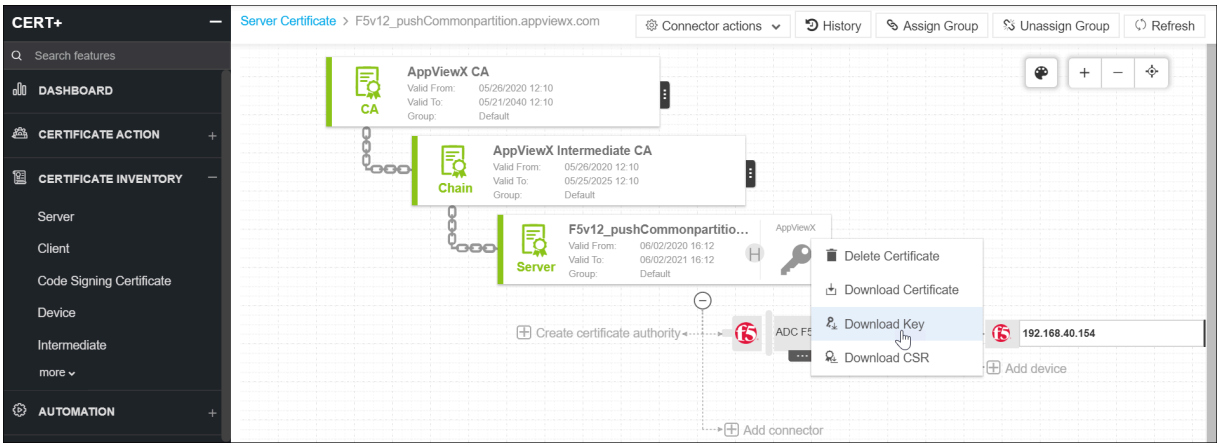
6. Click **Submit**.
7. On the screen that pops up, go to the key you want to upload and click **Open**.
   - If everything is correct, the key is uploaded to the certificate.
   - If the key you are trying to upload does not match the certificate, an error message appears on the top of the screen stating, **Certificate and key do not match**.

## Download a Certificate Key

> **Note:** This functionality is available only for server certificates.

To download a certificate key:

1. Click and select **CERT+** > **Certificate Inventory**.
2. Under **Certificate Inventory**, click **Server**.
3. On the Certificate Dashboard, click **List** on the top-right.
4. On the certificate list view, click the **Common Name** of the certificate to view the topology.
5. Hover over on the certificate and click**Download Key**.



6. On the **Download Key** pop up window, you can enter the password, enable key encryption, and choose between the **AE256** and **DES3** encryptions. Now, you can access the certificate key (after it is downloaded).

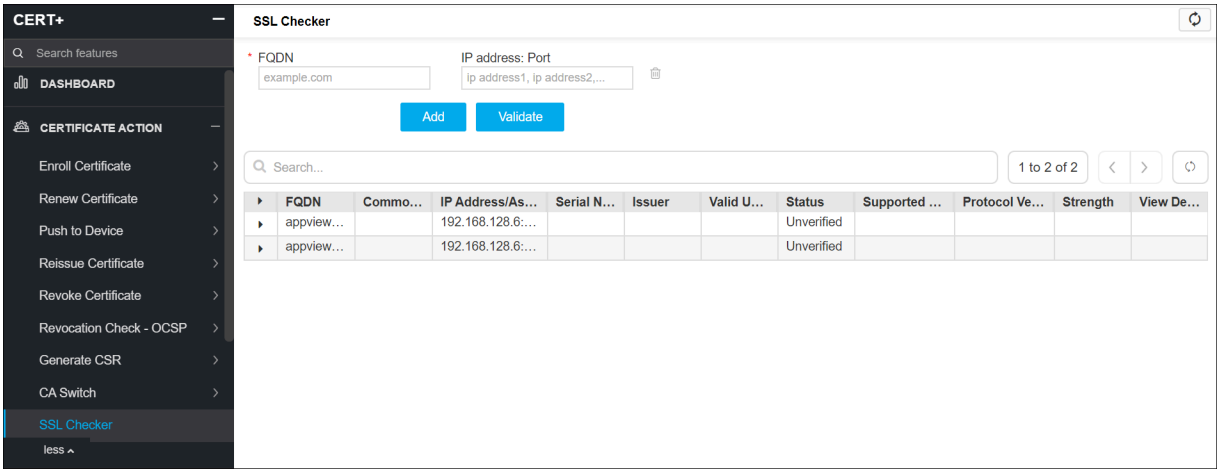
> **Note:** If you do not have the requisite permission to download the key, an error message appears on the top of the screen stating, **Private key access restricted**.

## Run SSL Checker on a Certificate

The SSL Checker feature in the Inventory module allows you to perform SSL checks and certificate validation on-demand by providing the fully qualified domain name (FQDN) or IP address and port of an SSL.

To run SSL checker on a certificate:

1. Click ☰ and select **CERT+** > **Certificate Action**.
2. Under **Certificate Action**, click **SSL Checker**.
3. On the SSL Checker details page, enter the Fully Qualified Domain Name (**FQDN**) for the SSL.
4. Enter the IP address and port for the SSL.
5. Click **Add** to add another **FQDN** and **IP address: Port** to the list of SSLs to be checked.
6. Click **Validate**.
7. If the SSL is valid, details appear on the table below.




## Add or Modify a Certificate Authority Account

To configure a certificate authority:

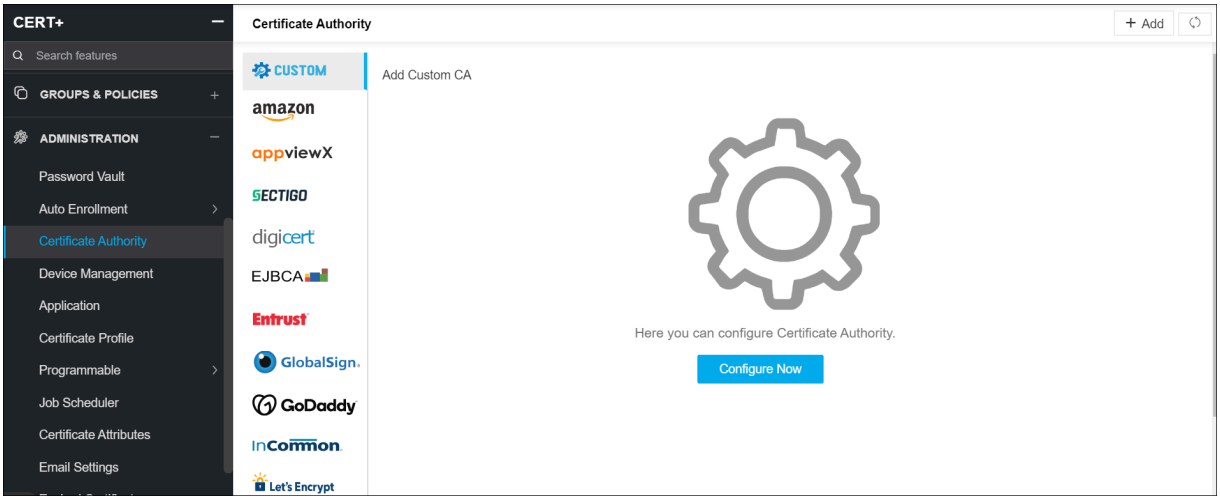
1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Certificate Authority**.
3. On the Certificate Authority page, a list of Certificate Authorities is displayed.
4. Click a vendor name to view the list of accounts configured for the selected CA.
5. Click + on the top-right.

> **Note:** Fields with a * are mandatory.

- Based on the details provided in the CA configuration, certificate product types can be fetched dynamically for **Sectigo** and along with divisions certificate product types can be fetched dynamically for **Digicert**.
- So, the certificate product types can be fetched dynamically for account details provided in the CA configuration.
- The **Fetch Custom Attributes** button is only available for the Entrust and Symantec CA(s). Click this button to connect to the corresponding CA account and retrieve the custom attributes from the CA portal.
- For **EJBCA CA**, there is a provision to validate the CA credentials and retrieve the certificate issuer name from the EJBCA account. Also, you can select the custom attributes configured in the EJBCA portal. The values for those custom attributes can be configured while submitting a CSR.
- For EJBCA custom attributes, State or Province, Country, Organization, and Organization unit values will be driven from policy and not from the CA settings to arrive at the compliance report using the custom attributes.
- When AppViewX CA needs to be configured for the first time, click the **Default AppViewX Setting** button to generate the Root and Intermediate CA.
- For Microsoft CA, the user can check/uncheck the CA manager approval option. When it is selected, it is mandatory to provide the manager's name and password. (When WMI is selected, Windows gateway should not be installed in the same CA machine.)

6. Click **Save**.
7. To edit account settings for a particular vendor, click that account. Fields corresponding to that account will be editable.
8. Make relevant changes and click **Update**.
9. To test the connection between the AppViewX and the CA account you created, click Check on the **Connection Status** column.

10. (Optional) Repeat steps 7 and 8 for other vendors whose CA details you wish to edit.



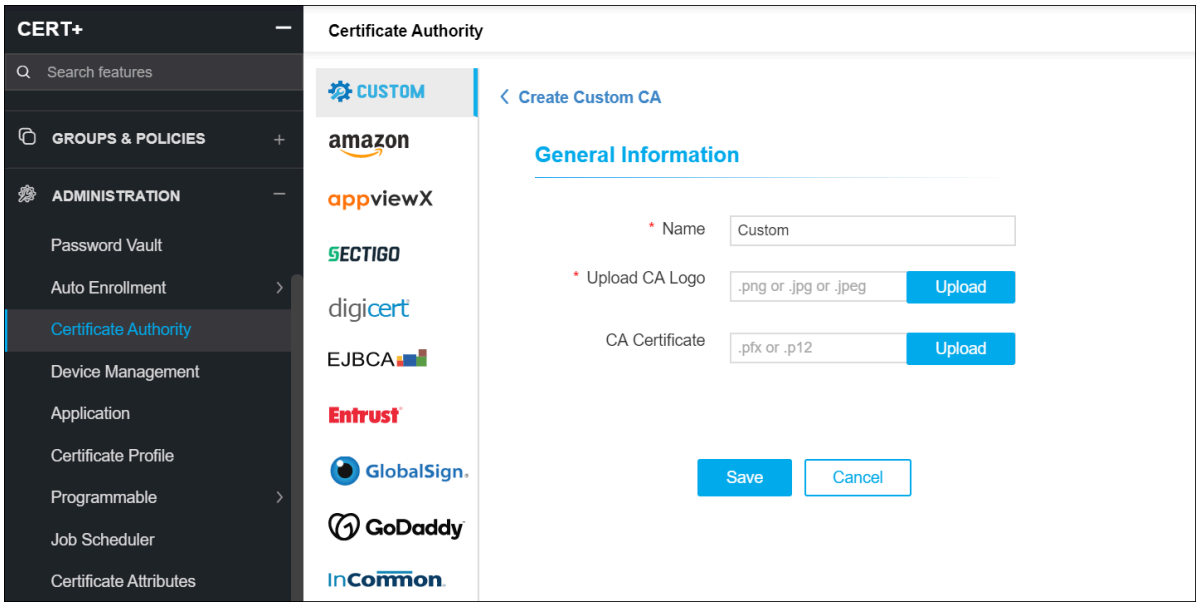

## Configure a Custom Certificate Authority

The Custom CA provides an option to create your own CA with the name of the corresponding organization or customer for which you want to create, rather than using the other CA(s).

To create a custom CA in AppViewX:

1. Click ☰ and select **Inventory** > **Certificate**.
2. The Certificate screen opens with the **Server** tab displayed by default.
3. (Optional) To create a custom CA for a client-vendor, click Client.
4. From the **Advanced** dropdown on the command bar, select the Settings option.
5. Click **Certificate authority** if it is not open already. The screen opens, listed on the left-hand column is the certificate authority (CA) available in AppViewX.
6. Click **Custom**.
7. On the screen that appears, enter a name for the CA you want to be displayed.
8. In the **Upload CA logo** field, click the **Upload** button to browse and navigate to the image you want to add and click **Open**.
   - The image will be displayed on the **Preview** field, click **Save**.
   - The newly created CA will be added to the vendor list in the left-hand column, where each CA is available in AppViewX. You must now create a root certificate for the new custom CA, under

which multiple intermediate CA(s) can be added. For more details, refer to **Create a Root and Intermediate Certificate Authority** .




## Add a Programmable Application Connector

**Note:** By default, the Windows JKS had been pre-configured.

To add a scripted application in AppViewX:

1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Application**.
3. On the Programmable Application page, click **+ Add** on the top-right.
4. Under the **General Information** section, in the **Name** field, provide a name for the new application connector to help users identify it.
5. From the **Purpose/Usage** dropdown, select the type of certificate from the list or if the list is extensive, use the search field in the dropdown to find.
6. In the **Upload Vendor Logo** field, click **Upload** to browse and go to the image you want to display on the server addition page. Click **Open**.
7. In the **Upload Vendor Icon** field, click **Upload** to browse and go to the image you want to display on the device inventory and holistic view. Click **Open**.
8. Select the **Windows** or **Linux** radio button depending on the type of server you want to use.
9. Under the **Application Configuration** section, provide the location of the Python script files (containing the actions to be performed on the templates) in the following fields:

- Discovery script
- Discovery script parameters
- Device Validation script
- Device Validation script parameters
- Pre - Push script
- Pre - Push script parameters
- Push script
- Push script parameters
- Post - Push script
- Post - Push script parameters
- Monitor script
- Monitor script parameters
- Rollback script
- Rollback script parameters

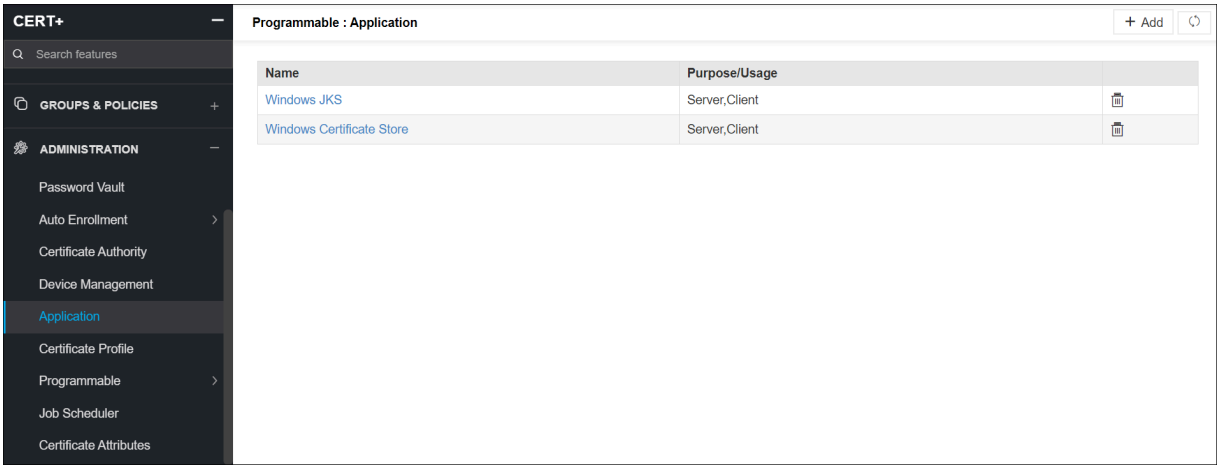
10. Click **Save**.

    The connector and its details are added and listed in the table at the bottom of the screen.

11. To edit settings for a particular application, click that connector.

    Fields corresponding to that connector will be editable.

12. Make relevant changes and click **Update**.



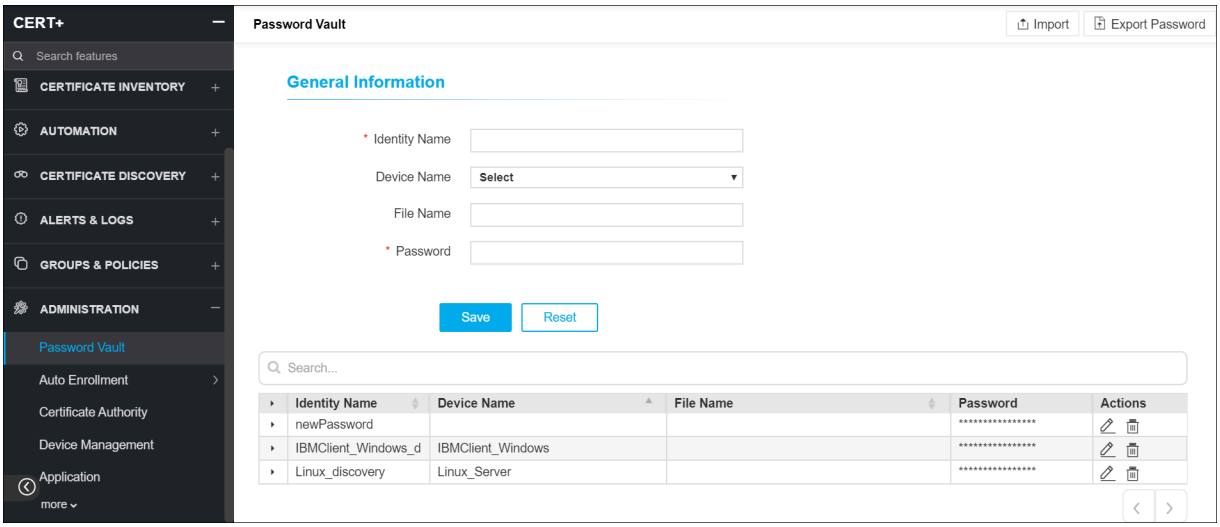

## Add a Password in the Vault

The password vault option is used to store all certificate passwords of the selected ADC devices. All the password-protected certificates that are discovered, will be decrypted and pushed to the discovery grid in the AppViewX Inventory. This happens only if passwords are matched with passwords that are stored in the vault.

**Note:** This functionality is supported only for the Citrix devices.

To add a password in the vault:

1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Password Vault**.
3. On the screen that appears, enter an **Identity Name** of the password you want to add in the vault.
4. From the **Device Name** dropdown, select the ADC device whose password-protected certificate details you want to store.
5. In the **File Name** field, enter a certificate file name to help users identify it.
6. In the **Password** field, enter the password that is associated with the certificate.
7. Click **Save**.
8. Click on the top-right to import a file (in XLS or CSV format) with a list of all certificate passwords. This option is used to store the certificate passwords directly in the vault instead of adding them manually.
9. Click on the top-right to export all stored certificate passwords from the vault as a zip file to your computer.

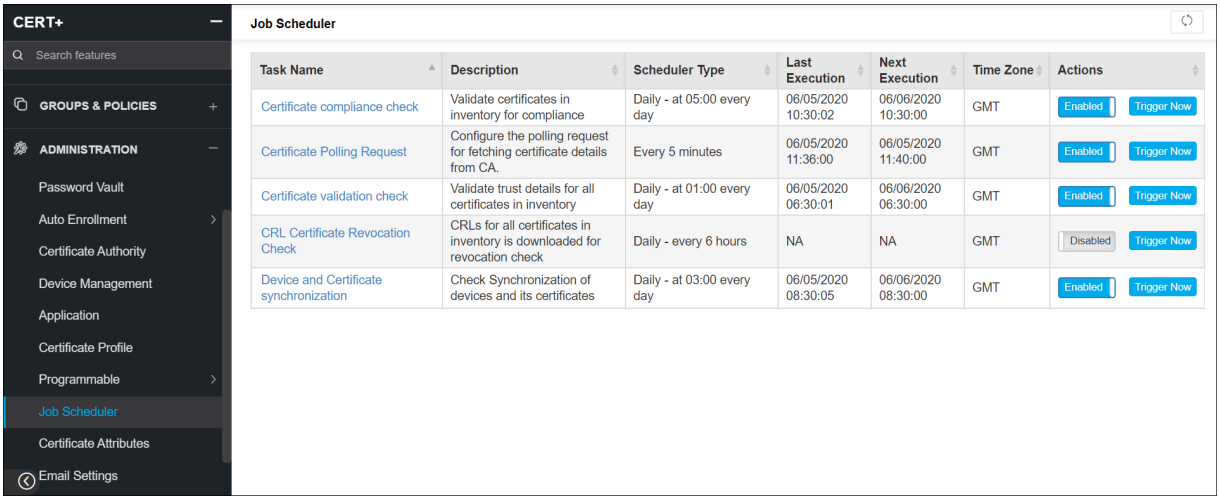



## Configure the Job Scheduler

To configure scheduled tasks:

1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Job Scheduler**.

3. On the Job Scheduler list view, you can enable/disable a particular task or trigger it immediately.




## Configure General Certificate Settings

To configure the generic settings:

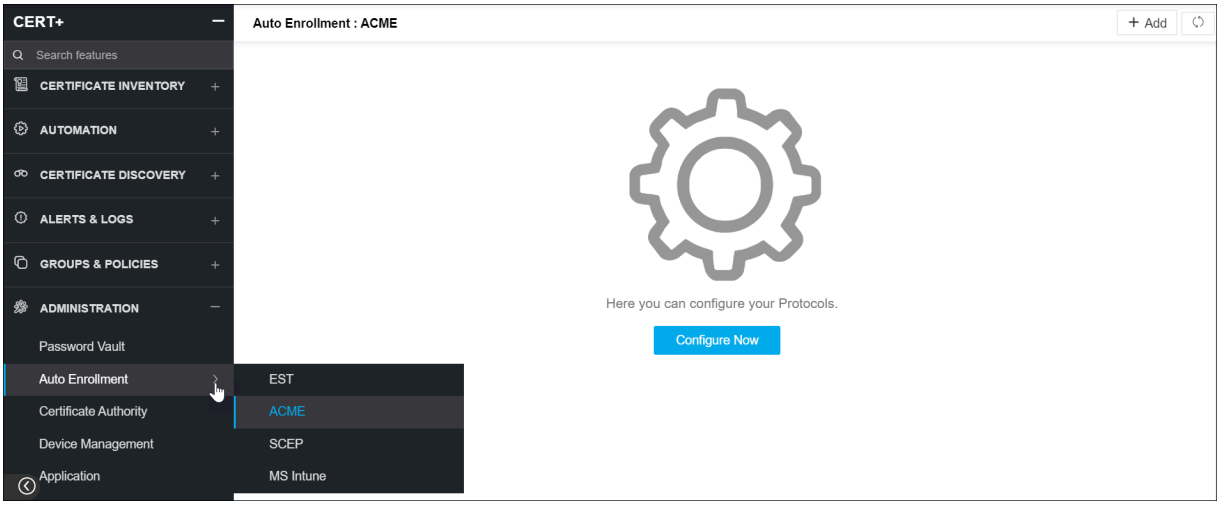
1. Click ☰ and select **CERT+** > **Administration**.
2. Under **Administration**, you can select one of the following tabs:
   - **Certificate Attributes** - On the screen that appears:
     - Click **Add New**.
     - On the **Certificate Attributes** pop up window, enter the **Key ID** and **Label Name** in the respective fields.
     - Click **Save**.
     - The newly created attribute is displayed on the table. From the **Actions** column, you can modify or delete an attribute.
   - **Email Settings** - Expand any task, fill email addresses for various levels of approvals and click **Save Changes**. You can click **+ Add** to include more keys and corresponding values to the task.
   - **Expired Certificates** - Select **Yes** (to delete expired certificates after expiry) and click **Save**.
   - **History of Certificates** - Select **Yes** (to maintain the history of a certificate after its renewal, reissue, or regeneration) and click **Save**.

## Configure Auto-Enrollment Settings

To configure the auto-enrolment protocol agents in AppViewX:

1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Auto-Enrollment**.
3. You can choose **EST**, **ACME**, **SCEP**, or **MS Intune** from the list.
4. Click **Configure Now**.
5. On the details page, enter the mandatory details and click **Save**.

> **Note:** For any protocol, more than one agent details can be added to AppViewX.



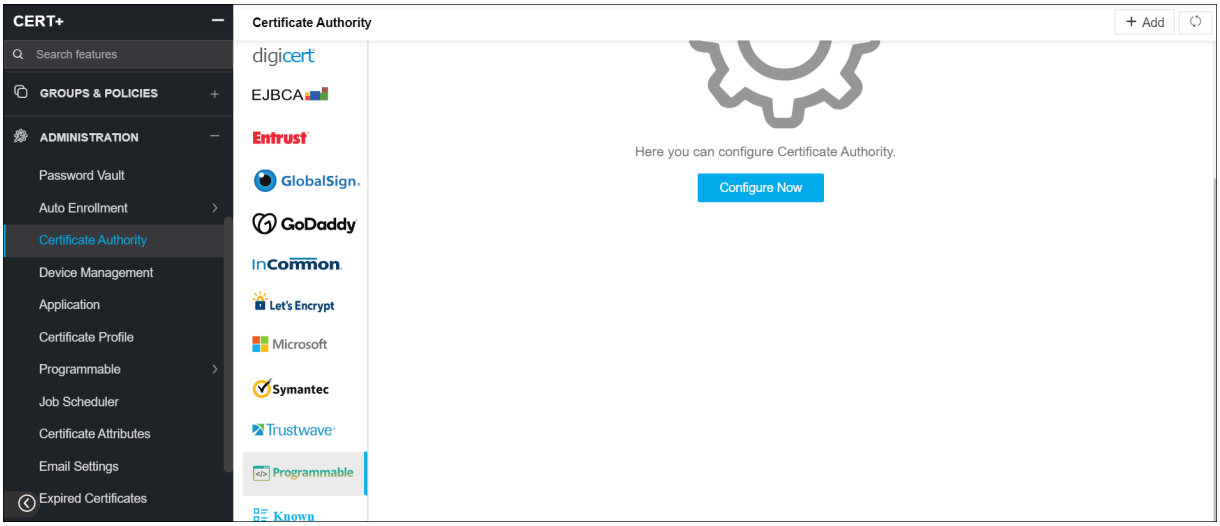

## Configure a Programmable Certificate Authority

To add a programmable certificate authority:

1. Click and select **CERT+** > **Administration**.
2. Under **Administration**, click **Certificate Authority**.
3. On the Certificate Authority page, a list of Certificate Authorities is displayed.
4. Scroll down to the bottom of the list and click **Programmable**.
5. Click **Configure Now** to create a new CA or click **Add** on the top-right to add another Programmable CA.
6. On the details page, under the **General Information** section, enter the information in the following fields:
   - In the **Certificate Authority** field, provide a name for the certificate authority.
   - Click **Upload** and browse the logo you want to add for the certificate authority.
   - In the **Name** field, provide a name for the new certificate authority to help users identify it.

- From the **Purpose/Usage** dropdown, select the type of certificate authority or if the list is extensive, use the search field in the dropdown list to find.
- (Optional) Select the **CSR Generation** checkbox if you want the CSR to be generated whenever you configure a CA.

7. Under the **CA Configuration** section, provide the location of Python script files (containing the actions to be performed on the templates) in the following fields:
   - CSR Submission Script
   - Fetch Script
   - Renew Script
   - Reissue
   - Revoke Script
   - CA Settings Parameters
8. Click **Save** to add the new certificate authority to the AppViewX system.

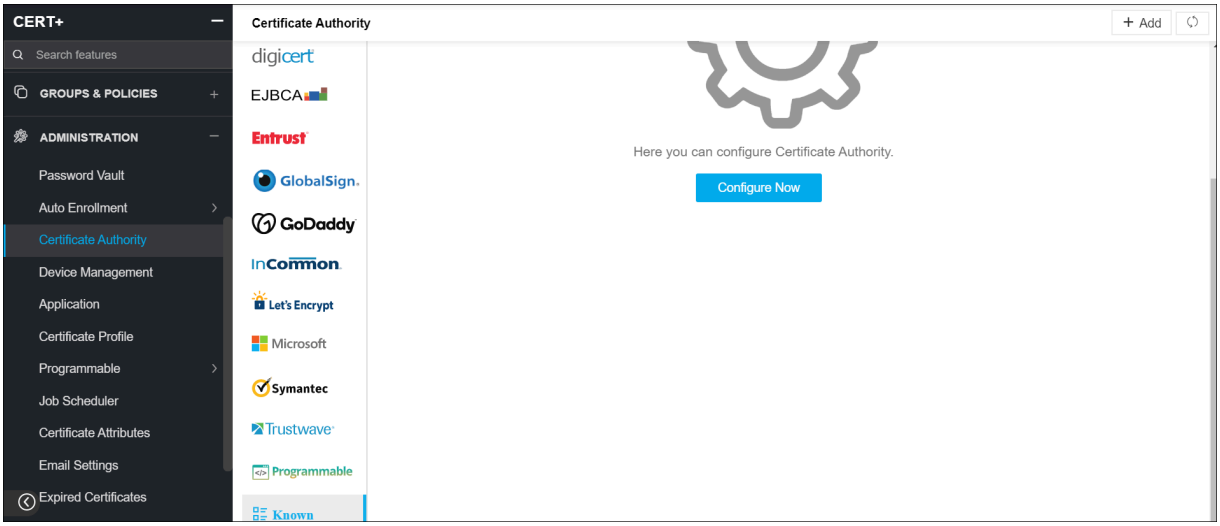



## Configure a Known Certificate Authority

To add or modify a known certificate authority:

1. Click ☰ and select **CERT+** > **Administration**.
2. Under **Administration**, click **Certificate Authority**.
3. On the Certificate Authority page, a list of Certificate Authorities is displayed.
4. Scroll down to the bottom of the list and click **Known**.
5. Click **Configure Now** to create a new CA or click **Add** on the top-right to add another Known CA.
6. On the details page, in the **CA Name** field, enter a name for the known CA.
7. From the **Root or Intermediate** dropdown, select the required certificate.

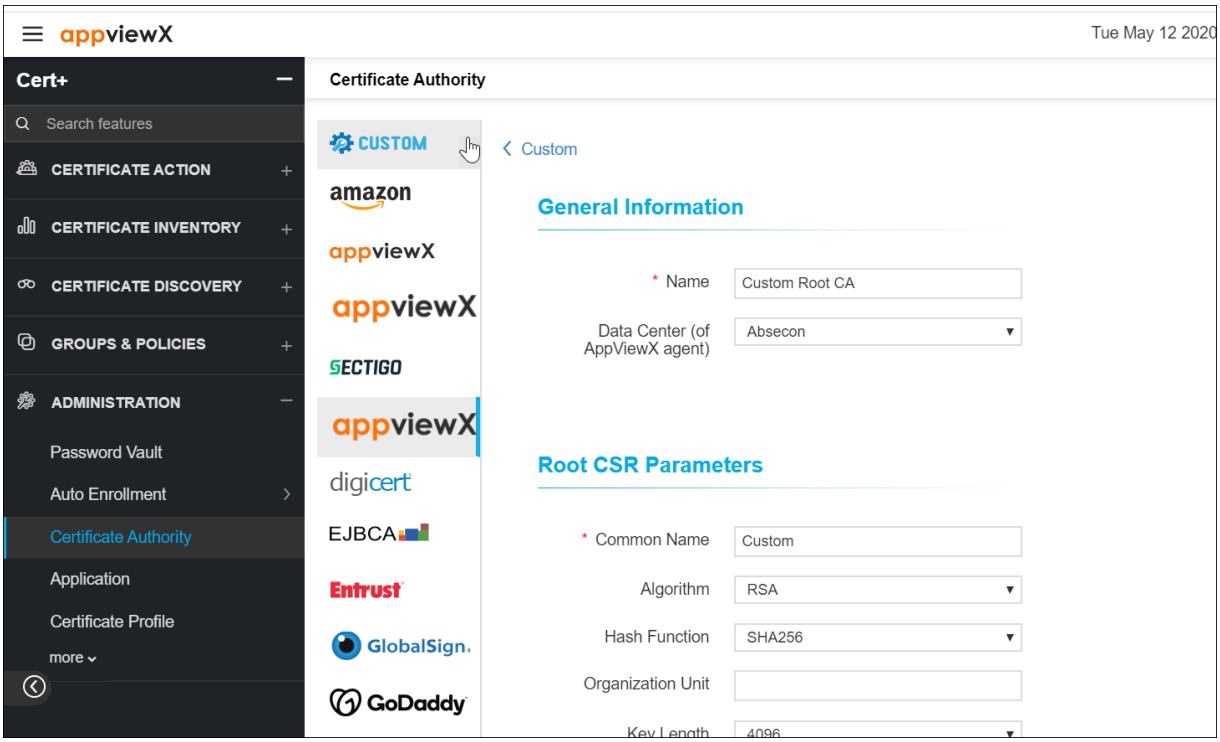
8. Click **Add**.




## Create a Root and Intermediate Certificate Authority

To create a root and intermediate certificate for the new custom CA:

1. Click ☰ and select **CERT+** > **Administration**.
2. Under **Administration**, click **Certificate Authority**.
3. On the Certificate Authority page, a list of Certificate Authorities is displayed.
4. Click **Custom** and create a new Custom CA.
5. Now, select the newly created Custom CA from the Certificate Authority list.
6. Click **Configure Now** or **+ Add** icon on the top-right of the page.
7. On the Custom CA details page, under the **General Information** section, enter a **Name** and **Datacenter**.
8. Under the **Root CSR Parameters** section, enter all Root CA fields with a red asterisk (*).




9. To add/configure from DigiCert and Microsoft Certificate Authority, credentials can be fetched from CyberArk.
10. Under the **Root Validity** section, enter the **Start Date** and **End Date**.
11. Click **Save**.
    The certificate topology screen opens.
12. Right-click on the root CA node and select **Submit** from the dropdown that appears.
13. On the Submit pop up screen, enter comments and click **Yes**.
    A request ID and work order ID are then generated automatically and the work order status is displayed beside the CA node as In Progress (Approval level 1). Right-click the CA connector and select Approve from the dropdown.
14. On the Implement screen that pops up:
    - Click ON to manually implement the request.
    - Click OFF to set auto-implementation. If you select this option, set the date and time that you want the implementation to occur.
15. Click **OK** to close the popup screen.
    he work order status updates to **In Progress** (CSR Submission). The request is then submitted for verification so that a root CA can be generated and retrieved by AppViewX. Depending on the CA, this process might take some time, in which case the work order displays a status of Awaiting CA Retrieval.
16. Click  on the command bar until the topology updates.

When the generated CA is successfully retrieved, a Chain of Trust displays on the topology and the status updates to Completed. The root CA that is generated will be displayed on the Custom CA collection grid.

17. Now, on the Custom CA screen when you click  on the command bar, the screen opens displaying all intermediate CA form fields.
18. Enter fields with a *.
19. Click **Save**.
    The certificate topology screen opens.
20. Right-click on the intermediate CA node and select **Submit** from the dropdown menu that appears.
21. On the Submit popup screen that appears, enter comments and click **Yes**.
    A request ID and work order ID are generated automatically and the work order status is displayed beside the CA node as In Progress (Approval level 1).
22. Right-click the CA connector and select Approve from the dropdown.
23. On the Implement screen that pops up:
    - Click ON to manually implement the request.
    - Click OFF to set auto-implementation. If you select this option, set the date and time that you want the implementation to occur.
24. Click **OK**.
    The work order status updates to **In Progress** (CSR Submission). The request is then submitted for verification so that an intermediate CA can be generated and retrieved by AppViewX. Depending on the CA, this process might take some time, in which case the work order displays a status of Awaiting CA Retrieval.
25. Click  on the command bar until the topology updates.
    When the generated CA is successfully retrieved, a Chain of Trust displays on the topology and the status updates to Completed. The intermediate CA that is generated will be displayed on the Custom CA collection grid.

## Create a CA Policy

To create a policy:

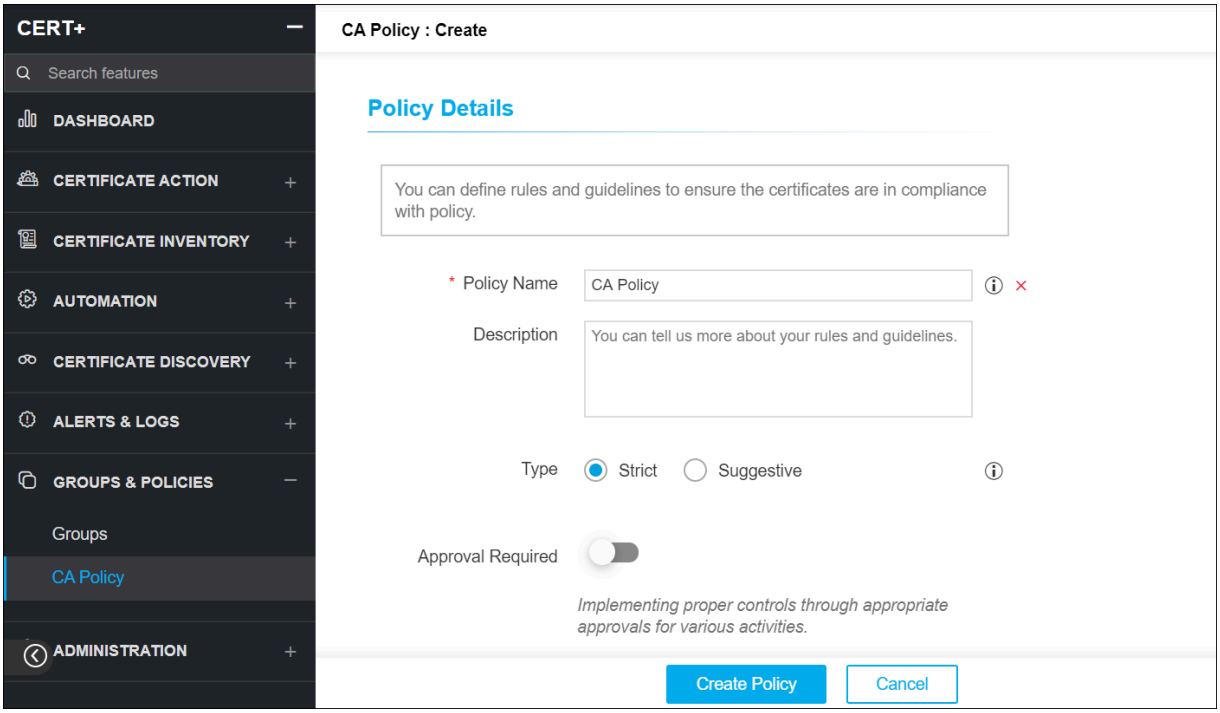
1. Click  and select **CERT+** > **Groups&Policies**.
2. Under **Groups & Policies**, click **CA Policy**.
3. On the **CA Policy** list view page, click **+ Create** on the top-right.
4. On the **Policy Details** page, enter a policy name.
5. In the Description field, enter the policy information.
6. Choose the **Policy Type** as Strict or Suggestive:

- Strict - While adding or updating the Certificate Authority (CA) connector, values provided as part of the Certificate Signing Request (CSR) information should match the values provided by the user in the policy. If the values do not match the policy, the user cannot save the CA connector details.
- Suggestive - While adding or updating the Certificate Authority (CA) connector, values provided as part of the Certificate Signing Request (CSR) information do not have to be an exact match to the values provided by the user in the policy. A user can modify the values provided, but the certificate is then considered to be non-compliant.

7. Enable **Approval Required** to implement proper control through appropriate approvals for various actions performed on the policy.
8. Enable **Private Key Access** option to allow the private key of the policy to be exported.
9. Enable **Include Root and Intermediate Certificates for Compliance Check** to perform a compliance check.
10. In the **CA Details** section, enter the following required information:
    - On the left pane, a window with a list of available Certificate Authorities is displayed.
    - Select the CA to associate the policy.
    - **Known CA List** - Choose any compliant Certificate Authorities.
11. **Certificate Parameters** section is optional and can be used later to help distinguish between multiple policies within the system.
    - Common Name - The fully qualified domain name (FQDN) or common name that exactly matches your web browser.
    - Organization - The name of the organization requesting the certificate.
    - Organizational Unit - The division of the organization requesting the certificate.
    - Locality - The location of the organization requesting the certificate.
    - State - The state in which the organization is located.
    - Country - The country in which the organization is located.
    - Email - The email contact details of the person responsible for maintaining the certificate.
    - Subject Alternative Name - Any additional hostnames, such as alternative websites, IP addresses, and so on, that have to be protected with the single SSL certificates.
    - Bit Length-Key Type - Choose the key length you want to generate and the key type depending on the type of security algorithm you want to use.
    - Hash Function - Select the hash function depending on the hash algorithm you want to use.
12. Under the **Group Selection** section, select the group(s) you want to include in the policy or create a new group to which the policy must be assigned.

**Note:** You can search for the required group and add the frequently used keywords as favorites.

13. Under the **Compliance Check** section, you can enable the **Perform Compliance Check** option if the respective policy that you have configured is compliant.
14. Click **Create Policy**.



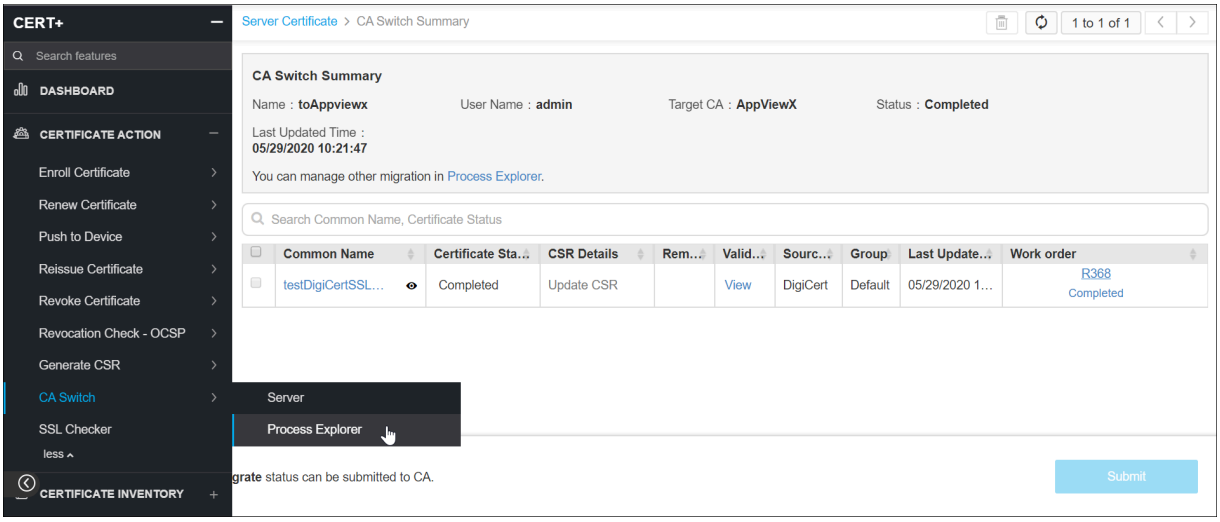

**Note:** If you want to make any changes to the policy in the future, you can select the policy and make the respective changes. If you want to completely reset the policy data, click the **Reset** icon beside the CA name on the right pane as shown in the below image.

## View the Process Explorer

To modify the CA switch of a certificate:

1. Click and select **CERT+** > **Certificate Action**.
2. Under **Certificate Action**, click **CA Switch>> Process Explorer**.
3. On the CA Switch list view page, you can view the list of certificates that were switched or up for switching.

4. Click the **Name** of a certificate to view it's **CA Switch Summary** details.




# SSH Tasks

- Overview
- Discover an SSH Key
- View SSH Key Details
- View the Different Statuses and States for an SSH Key and Host
- View SSH Host Details
- View SSH Policy Details
- Create an SSH Key
- Create an SSH Host
- Create an SSH Policy
- Push an SSH Key from a Connector
- Modify an SSH Key
- Modify an SSH Host
- Modify an SSH Policy
- Upload an SSH Key
- Fetch Keys for an SSH Host
- View the Device Status Log for an SSH Host
- Associate a Client Device with an SSH Key
- Associate a Server Device with an SSH Key
- Modify an SSH Key Connector

- Update a Known Host File
- Set Up Privileged Access Management for an SSH Host
- Delete an SSH Key from a Connector
- Delete an SSH Key from a Device
- Delete an SSH Key from the Database
- Delete an SSH Host
- Delete an SSH Policy
- Change the Status of an SSH Key
- Assign or Unassign a Group to an SSH Key
- Export an SSH Key
- Export an SSH Host
- Download a Public SSH Key
- Download a Private SSH Key
- Rollback an SSH key
- Rotate an SSH Key
- Renew an SSH Key
- Refresh the Component
- Retry a Failed Workorder
- Monitor SSH Sessions

## Overview

AppViewX SSH+ is a web-based SSH key management solution offered to Linux support systems that allow password-less authentication between Linux machines using public and private keys. SSH+ offers the following:

- Automated key discovery and inventory through the use of a discovery scanner that identifies new SSH key pairs and provides a single centralized repository for user-defined SSH key management.
- A centralized repository of the SSH keys and Host that are discovered.
- A holistic view of SSH keys and Hosts against end-user mappings.
- Role-based access control (RBAC) with granular access for ease of administration.
- Audit and compliance capabilities.
- A scalable architecture to support cloud-based hosts, thereby providing complete visibility and access control to the security managers.

## Discover an SSH Key

The Discover function allows you to search for and display the list of all available SSH keys.

**Note:** Discovery is not supported for F5 (ADC) devices.

To discover an SSH key, complete the following steps:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed by default, click to open it.
4. Click in the Command bar.
5. On the Discover screen that opens, select whether you want key discovery to happen immediately (Instant) or at a specific time in the future (Scheduled).

   **Note:** Click to view the defined discoveries (in the AppViewX Config file) that were triggered at midnight. All those discoveries of managed devices will be displayed in a table format.

6. If you selected Instant in Step 5, jump to Step 7. If you selected Scheduled, enter the following details in the Scheduler region that appears:
   - Schedule name - Enter a name that clearly identifies the scheduled key discovery action that you are setting up.
   - Description - Enter a description of the scheduled key discovery that makes it easy for a reader to immediately determine when the key discovery is scheduled to take place.
   - Recurrence Type - Select the frequency of the key discovery process: once, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on what you select here. At a minimum, complete all fields designated with a red asterisk (*).
   - Time - Set the specific time you want key discovery to take place.
   - Date - Select the date that you want key discovery to take place, or for recurring discoveries, the start and end dates that you want key discovery to begin and end respectively.
7. In the Discovery name field, enter a name for the discovery so that you can identify it later as needed.
8. In the Description field, enter a description of the discovery that makes it easy for a reader to immediately determine which key is being discovered.
9. In the Discovery Mode field, select the means by which you want to discover the SSH key:

- Managed devices - If you select this option, complete the following sub-steps:
  a. Select each of the managed devices you want to use in the discovery process.
  b. Select the required condition and lick the Add as Regex button; then, jump to step 12.
- IP range - If you select this option, complete the following sub-steps:
  a. Enter a starting IP address and an ending IP address to define the IP range you want to use.
  b. Select the port or ports you want to use.
  c. From the **Credential Type** dropdown, select one of the following options:
    - **Manual Entry** - You must provide the credentials for device communication and all the SSH operations.
    - **Credential List - AppViewX** - The active credentials in the system are listed. You can select the required credentials and assign them for SSH host and all the other SSH operations.
    - **Credential List - CyberArk** - The AppViewX system communicates with CyberArk and retrieves the passwords for all the SSH operations.
  d. Select the Login Type you want to use to access the IP range: Password, which requires a username and password combination, or Identity key, which requires a username and identity key and, in some cases, a passphrase. Then, jump to step 10.
- Subnet - If you select this option, complete the following sub-steps:
  a. Enter the network containing the subnet you want to use for discovery.
  b. Select the port or ports you want to use.
  c. From the **Credential Type** dropdown, select one of the following options:
    - **Manual Entry** - You must provide the credentials for device communication and all the SSH operations.
    - **Credential List - AppViewX** - The active credentials in the system are listed. You can select the required credentials and assign them for SSH host and all the other SSH operations.
    - **Credential List - CyberArk** - The AppViewX system communicates with CyberArk and retrieves the passwords for all the SSH operations.
  d. Select the Login Type you want to use to access the IP range: Password, which requires a username and password combination, or Identity key, which requires a username and identity key and, in some cases, a passphrase. Then, jump to step 10.
- Cloud - If you select this option, complete the following sub-steps:

**Note:** Make sure that you set the cloud based key discovery method either by using private IP or public IP. For more details refer to the SSH settings section of this guide.

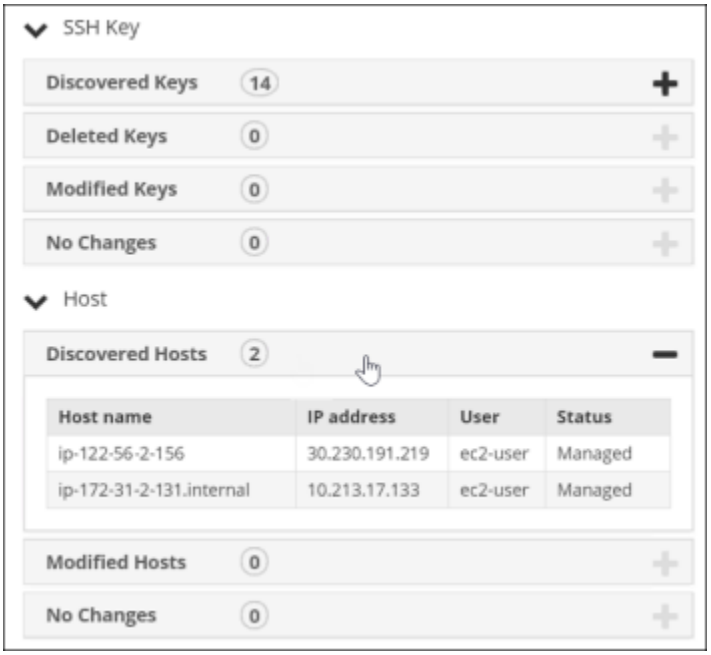
a. In the Cloud Vendor field, select the vendor whose devices you want to run a discover operation for.
b. In the Account Name field, select the cloud vendor account you want to run a discover operation for.AppViewX will authenticate the account based on the cloud vendor and account you selected. After the authentication is successful, it will display the respective fileds by which fetch instance is triggered.
c. Click the Fetch Instance button to have the system grab all instances that exist for the account you specified in Step b.
d. Select all instances or any of the instance that you want to discover from the results field that appears beneath the Fetch Instance button, then click the **Add as Regex** button.
e. The **Regex** column displays the total number of keys that match each of the regex search criteria you have created.
f. Select the port or ports you want to use.
g. From the **Credential Type** dropdown, select one of the following options:
   - **Manual Entry** - You must provide the credentials for device communication and all the SSH operations.
   - **Credential List - AppViewX** - The active credentials in the system are listed. You can select the required credentials and assign them for SSH host and all the other SSH operations.
   - **Credential List - CyberArk** - The AppViewX system communicates with CyberArk and retrieves the passwords for all the SSH operations.
h. Select the Login Type you want to use to access the IP range: Password, which requires a username and password combination, or Identity key, which requires a username and identity key and, in some cases, a passphrase.
i. Select the **Sudoer User** checkbox to provide admin access to the user.
j. In the Username field, enter the name of the user who has access permissions for the account you selected in Step b.
k. Enter the password for the account you selected in Step b. Then, jump to step 10.

10. In the Host Group and Key Group fields, select the host group and key group that that you want the keys you discover to be associated with.
    The policy associated with the groups will automatically be associated with the keys that are discovered.
11. Select the Manage or Monitor radio button depending on what you want to do with the keys you discover.
12. Click Discover (if you selected Instant in Step 5) or Save (if you selected Scheduled).The table at the bottom of the screen updates to show the details of the immediate or scheduled discovery action.
13. Click the name of one of the completed discovery operations in the table.

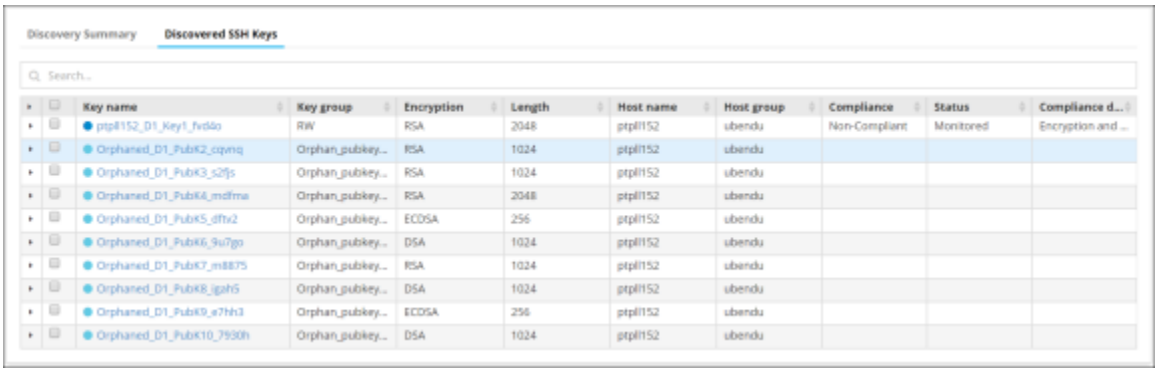
The Discovery screen that appears contains two tabs: Summary and Discovered SSH Keys.The Discovery Summary tab displays the parameters that you set for the discovery operation along with the following statistics:

- Number of discovered keys
- Number of deleted keys
- Number of modified keys
- Number of keys with no changes
- Number of discovered hosts
- Number of modified hosts
- Number of hosts with no changes

14. Click ✚ in any of the statistics rows to expand the row to display the names of the related keys or hosts. If there are no entries for a particular row, the Expand icon is grayed out, as shown below for the Deleted Keys, Modified Keys, No Changes, Modified Hosts, and No Changes rows.




15. Click  to view the status of the host devices and  to go back to the previous screen again. The Discovered SSH Keys tab displays full details for all SSH keys that were discovered.




16. Click any of the links in the Name column to view the holistic view of the related SSH key.

## View SSH Key Details

There are two places where you can view SSH key details and each provides slightly different information about the key.

## View Details on the SSH Key Tab

To view the details for an SSH key via the SSH Key tab:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed, click to open it.
4. If the SSH key whose details you want to view is not visible on the screen, use the Search field to locate it.
   The following details appear for each SSH key:
   - Key name
   - Key group - Includes information as to whether the group has Read-Only or Read/Write access to the key.
   - Encryption type - RSA, DSA, or ECDSA
   - Encryption bit length - Varies depending on the selected encryption type
   - Age of the key
   - Created by - Creator of the key
   - Client machines associated with the key
   - Server machines associated with the key
   - Compliance status - Compliant or Non-compliant

- Key status - Managed or monitored
- Associated users
- Compliance description - Indicates whether the encryption and the bit-length parameter are compliant or non-compliant

## View Details from the SSH Key Holistic View

To view SSH key details from the SSH key holistic view:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed by default, click to open it.
4. If the SSH key whose details you want to view is not visible on the screen, use the Search field to locate it.
5. On the SSH key topology that opens, click » on the side of the screen.


The details panel that appears lists the following information about the key:

- Key name
- User name
- Key creation date
- SSH Key group
- Any comments associated with the key
- Encryption type and length
- Key validity duration
- The compliance status of the key
- Key status
- Rotation time for the key
- Rotate automatically setting: enabled or disabled
- Push automatically setting: enabled or disabled
- Last rotate time
- Next auto-rotate time

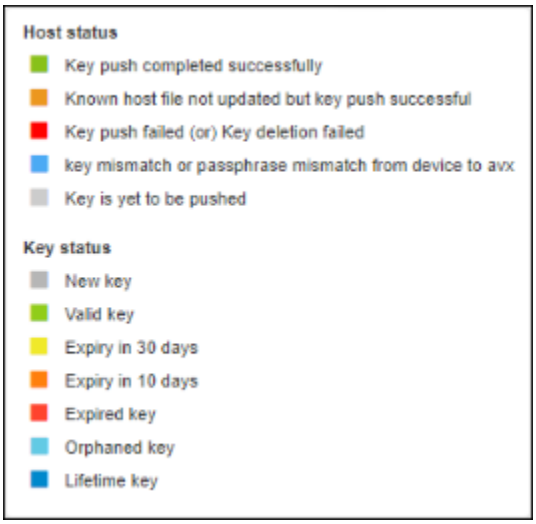
- Key expiry date
- Last renewal date

**Note:** The details panel also contains a search field that allows you to search for any other SSH key without returning to the main SSH Key screen.

## View the Different Statuses and States for an SSH Key and Host

To see a list of all of the statuses an SSH key can have:

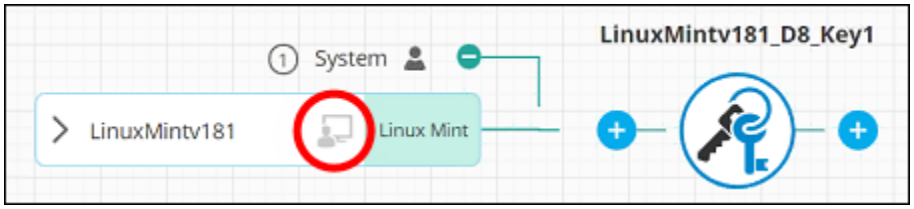
1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed by default, click to open it.
4. Click any of the key links in the Key name column.
5. In the key holistic view that opens, click .
   A legend appears, listing each of the possible SSH key/host statuses and states.




   Using this legend, you can tell at a glance the current status and state of a key and its host. In the example below, for example, the key is blue, indicating that it is a Lifetime key that does not expire.

   The following are the various color code indications for the known host file update:

- • The host icon (circled) is gray, indicating that the key has not been pushed to the device.




  - The host icon (circled) is orange, indicating that the known host file has not been updated even after the key is successfully pushed to the device.
  - The host icon (circled) is blue, indicating that the known host file has not been updated and the key mismatch.
  - The host icon (circled) is green, indicating that the known host file has been updated and the key pushed to the device.

## View SSH Host Details

To view the details of an SSH host:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the Host tab to open it.
4. If the SSH host whose details you want to view is not visible on the screen, use the Search field to locate it.
5. The following details appear for each SSH host:
   - Hostname
   - IP address - Clicking on this will display the SSH keys that are discovered and pushed to the device from the logged-in user account.
   - Device name
   - Host group
   - Vendor
   - Version
   - Category
   - Host status - Clicking on the state of the required host in this column will display the following details in the **Device status log** window:

**Note:** You can click + on the left-hand side of the required detail for more information. Also, the overall status of the device is displayed next to the detail.

- Device communication
- Pre-requisite checks on SSH hosts
- Midnight key sync
- Fetch key

**Note:** If the device communication or the prerequisite check fails, then the status is set to be "unmanaged, unresolved, or failed". The SSH operations cannot be performed on an unmanaged device.

- User
- Port
- Detailed Version

## View SSH Policy Details

To view details of an SSH policy:

1. Click ☰.
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the Policy tab to open it.
4. If the SSH policy whose details you want to view is not visible on the screen, use the Search field to locate it.
5. The following details appear for each SSH policy:
   - Policy name
   - Key group associated with the policy
   - Type of policy
     - Strict - Strict policies require that the encryption values and the bit length of the SSH key exactly match those of the policy. If they do not, the request fails.
     - Suggestive - Suggestive policies do not require that the encryption values and the bit length of the SSH key exactly match those of the policy.
   - Description

- To see additional details about the policy, click  in the Command bar.
- The Modify screen that appears displays the current settings for the policy, including the following fields that are not visible on the main SSH policy screen:
  - Private key access - If selected, gives authorized users the ability to access and download the private key
  - Enforce Key Approval WO - Create and delete SSH keys with approval work order
  - Encryption type - RSA, DSA, or ECDSA
  - Bit length - Varies depending on the encryption type that was selected

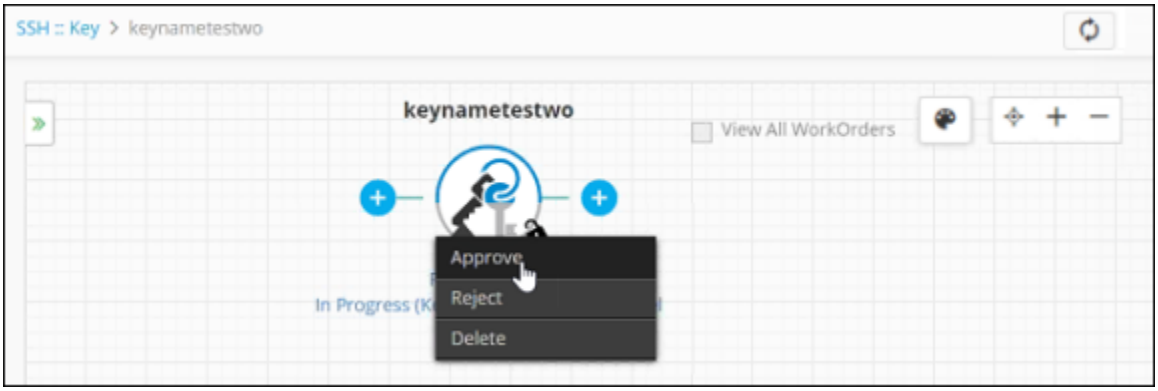
## Create an SSH Key

The steps involved in creating an SSH key differ depending on whether or not the key is associated with a key policy that requires work order approval and implementation of all actions initiated on the key. The instructions below cover both of these possibilities.

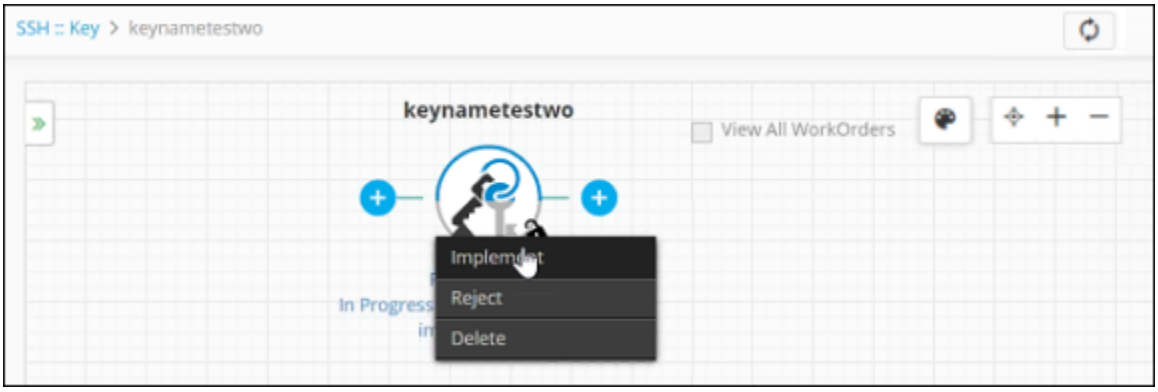
To create an SSH key, complete the following steps:

1. Click  and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. Click  in the Command bar.
4. On the Generate SSH Key screen that appears on the right side of the screen, select the Key group that you want to create an SSH key for.
5. Enter a name for the new SSH key.
6. (Optional) Enter and confirm a passphrase for the key.
7. Select the type of encryption you want the new key to use: RSA, DSA, or ECDSA.
8. Select the bit length you want for the encryption. The options in this field vary depending on the type of encryption you selected in Step.
9. Select how long you want the key to be valid: Lifetime, Days, or Years.
10. If you selected Lifetime in Step 10, jump to Step 12.
11. If you selected Days or Years in Step 10, in the Validity field, specify exactly how many days or years the key should be valid. After the validity expires, the keys will be deleted from the associated host (client and server).(Optional) Enter any comments you want related to the SSH key you are creating.
12. The Push automatically toggle is enabled by default. If you want to disable automatic pushing of the key to any new connectors that are associated with the key, click  to switch it to  .
13. The Rotate automatically toggler is disabled by default. If you want to enable automatic rotation of the SSH key for security compliance reasons, click  to switch it to  .

14. Click **Generate** to create the SSH key.
    If the key policy does not require work order approval, then the key creation process is complete. If the key policy does require work order approval, the process continues through the following steps.
15. The key then appears in a holistic view. Right-click the key and select Approve from the dropdown menu that appears.




16. On the Approve popup screen that appears, enter any comments you have about the creation, then click **Yes**.
17. Click  in the holistic view to refresh the screen until the key shows the status of Key Creation - Awaiting implementation.
18. Right-click the key and select Implement from the dropdown menu that appears.




19. On the Implement screen that pops up, enter any comments about the implementation, then click **Yes**.

20. Click  in the holistic view to refresh the screen until the key shows the status of Key Creation - Completed.


## Create an SSH Host

To create an SSH host:

1. Click  .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the Host tab to open it.
4. Click  in the Command bar.
5. On the Create screen that appears in the bottom-right corner of the screen, select the Host group that you want to create an SSH host for.
6. In the Device name field, enter a name for the machine that you want to use as an SSH host.

> **Note:** You can add an ADC device (only F5 and HA proxy vendors are supported) only through the device inventory, and it can be modified through the SSH host.

7. In the **Communication** field, select one of the following options:
   - In the IP address field, enter the IP address of the host machine.
   - In the **FQDN** field, enter the fully qualified domain name of the SSH host.
8. In the Port field, leave the default setting of 22, or select the Custom radio button and then enter a different port number in the field below.
9. From the **Credential Type** dropdown, select one of the following options:

- **Manual Entry** - You must provide the credentials for device communication and all the SSH operations.
- **Credential List - AppViewX** - The active credentials in the system are listed. You can select the required credentials and assign them for SSH host and all the other SSH operations.
- **Credential List - CyberArk** - The AppViewX system communicates with CyberArk and retrieves the passwords for all the SSH operations.

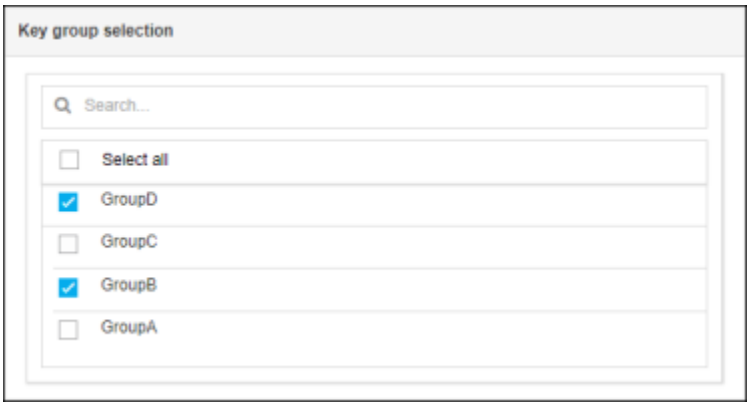
10. In the Login using field, select whether you want users to log in to the machine using a password, in which case you must enter the password in the field below, or using an identity key, in which case you must choose the key and enter the passphrase in the fields that appear below.
11. Hosts should be added only with the root user credentials who can access all the files. Also, in the **Credentials** pane, users should select **sudo** or **dzdo** from the **Access Elevation** section.
12. In the Username field, enter the username that has permission to access the device you listed in Step 6.
13. In the Password field, enter the password that is associated with the user you listed in Step 10.
14. Click **Save** to create the SSH host.

## Create an SSH Policy

To create an SSH policy, complete the following steps::

1. Click  .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the **Policy** tab to open it.
4. Click  in the Command bar.
5. On the Add screen that appears, select one of the following types of policy:
   - **Key** - Enter a name for the policy and follow step 7 onwards.
   - **Host** - Enter a name for the policy and select a vendor (F5 or Linux) of your choice from the left side. Then, configure the parameters as per your liking and jump to step 15.
6. Select the type of policy you want to create:
   - Strict - Strict policies require that the encryption values and the bit length of the SSH key exactly match those of the policy. If they do not, the request fails.
   - Suggestive - Suggestive policies do not require that the encryption values and the bit length of the SSH key exactly match those of the policy.
7. Enter a description of the policy that makes it easy for users to tell what the policy covers.
8. Select the Private key access checkbox if you want to give authorized users the ability to access and download the private key.

9. Select the Enforce Key Approval WO checkbox if you want to have a work order generated automatically for any key that uses this policy whenever an action is initiated on the key. If you do not select this option, then actions initiated on keys that use this policy are approved and implemented automatically.
10. Select the encryption type you want to use for the policy: RSA, DSA, or ECDSA.
11. Select the bit length you want to use for the encryption type. The values in this field vary depending on the type of encryption you selected in Step 9.
12. In the Key group selection field, select each key group that you want to associate with the policy you are creating.




13. Click **Create** to finish creating the policy.

## Push an SSH Key from a Connector

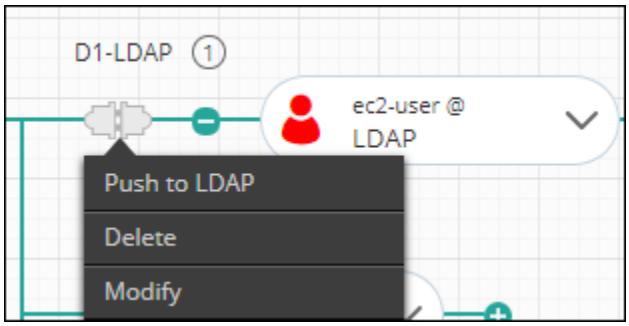
## For LDAP and Azure

To push an SSH key to a device:

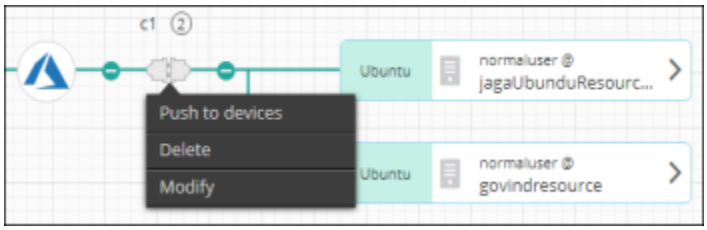
1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed, click to open it.
4. Use the **Search** field to locate the SSH key you want to delete.
5. Click the link in the Key name column for the key you want to delete. The holistic view appears, with the SSH key displayed.
6. Right-click option varies based on the connector type. Select one of the following to which you want to push the SSH key:

**Note:**
Push to LDAP option allows the LDAP directory to push the public key to the associated instance of the user through the scripts.

- LDAP connector type - Right-click the **Connector** and select Push to LDAP from the menu that appears.




- Azure connector type - Right-click the **Connector** and select Push to device from the menu that appears.




7. On the screen that pops up, click **Yes** to confirm that you want to push the key to the device.
8. If the key policy does not require work order approval, then the key push process is complete.
9. If the key policy does require work order approval, the process continues through the following steps. On the holistic view screen, the key status changes to In Progress (Approval level 1).

**Note:** You might have to click a few times to update the screen to see the status change.

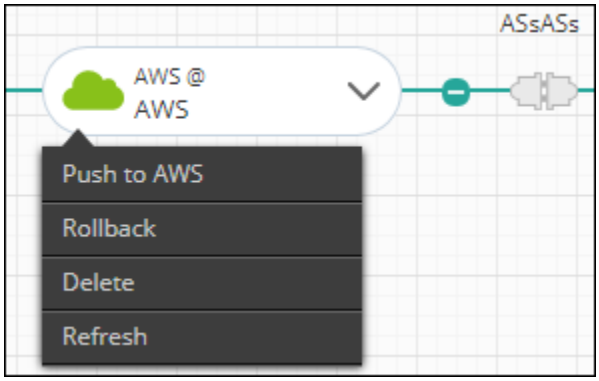
10. Right-click the connector and select **Approve** from the dropdown menu that appears.
11. On the Approve popup screen that appears, enter any comments you have about the key push approval process, then click Yes.
12. Click in the holistic view to refresh the screen until the key shows a status of In Progress (Awaiting implementation).
13. Right-click the connector and select Implement from the dropdown menu that appears.

14. On the Implement screen that pops up, enter any comments about the implementation, then click **Yes**.
15. Click  in the holistic view to refresh the screen until the key shows the status of Push - Completed.

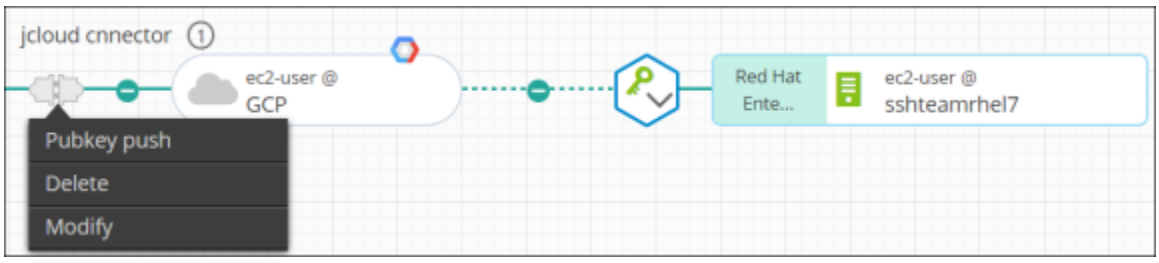
## For AWS and GCP

To push an SSH key to a device, complete the following steps:

1. Complete steps 1 to 6 in the above procedure.
2. Right-click option varies based on the connector type. Select one of the following to which you want to push the SSH key:
   - **AWS Connector Type**
     - Right-click the **AWS inventory** and select Push to AWS from the menu that appears.



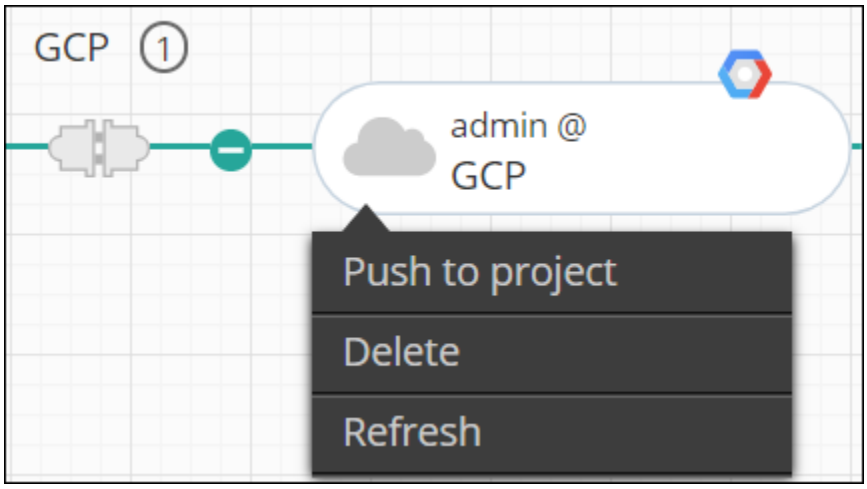

     - Right-click the AWS inventory and select **Push to devices** from the menu that appears.
     - From the Push to devices screen that appears, select one of the following options:
       - **Push Public key to associated instance (default)**
       - **Push Public key to associated AWS account inventory**
       - **Push Public key to both (associated instances and AWS account inventory)**
   - **GCP Connector Type**
     - Right-click the connector before GCP inventory and select **Pubkey push** from the menu that appears.



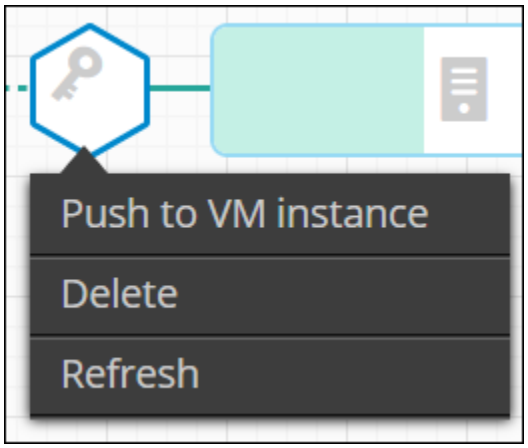

     - Right-click the GCP inventory and select **Push to project** from the menu that appears.
     - From the Pubkey push screen that appears, select one of the following options:

- **Push Public key to Google account inventory**
- **Push Public key to associated Instance property**
- **Push Public key to both (associated instance property and Google account inventory)**

3. Alternatively, you can also complete the following steps:
   - Right-click the Google inventory and select **Push to project** from the menu that appears.




   - Right-click the Google instance and select **Push to VM instance** from the menu that appears.




   - (Optional) In the **Comments** box, add additional information and click **Yes**. Complete steps 7 to 13 in the above procedure.

## Modify an SSH Key

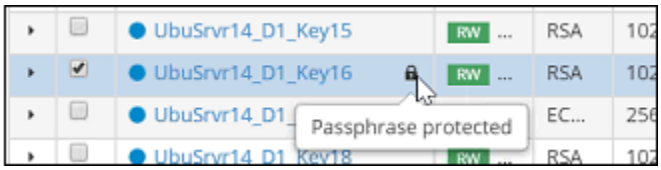
In order to modify an SSH key, it must have a status of Managed, which you can tell by looking in the Status column for the key details. If the key has a status of Monitored, you must change it to Managed using the steps outlined in the Change the Status of an SSH Key section of this guide.

To modify an SSH key:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed by default. Click to open it.
4. Select the checkbox beside the SSH key that you want to modify.

> **Note:** You can tell at a glance if a key has passphrase associated with it by looking for a lock icon beside its name.

5. Click in the Command bar.
   If an SSH key has a passphrase associated with it, you are prompted to enter the passphrase when you click the key link. If no passphrase is associated, the Modify screen appears immediately.




6. On the Modify screen that appears in the bottom-right corner of the screen, you can modify any of the following key details:
   - Passphrase
   - Validity: The timespan the key is valid, expressed in days or months, or lifetime
   - Push automatically: Toggle between enabled and disabled
   - Rotate automatically: Toggle between enabled and disabled
   - TTL (time-to-live): The number of hours or days you want the key to be active before it gets rotated out
7. Click **Update** to save your changes.

## Modify an SSH Host

To modify an SSH host:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the **Host** tab to open it.
4. Select the checkbox beside the SSH host that you want to edit.
5. Click in the Command bar.

6. On the Modify screen that appears in the bottom-right corner of the screen, modify any of the host details you want, other than the Host group field, which cannot be edited.
7. Click **Update** to save your changes.

> **Note:** When you modify the F5 and HA proxy ADC devices, there is an option to use the credentials which you had added while creating a device.

## Modify an SSH Policy

To modify an SSH policy:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Policy tab is not displayed, click to open it.
4. In the list of SSH policies, select the checkbox beside the policy you want to modify.
5. Click in the Command bar.
6. On the Modify screen that appears, modify any of the policy details you want, other than the Policy name field, which cannot be edited.
7. Click **Update** to save your changes.

## Upload an SSH Key

To upload an SSH key:

1. Click .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. If the Key tab is not displayed, click to open it.
4. Click in the Command bar.
5. On the Upload SSH key screen that appears in the bottom-right corner of the screen, click that appears in the Key File field, locate the SSH private key you want to upload, then click Open to add its file path to the Key File field.
6. Select the Key group that you want the uploaded SSH key to belonging to.
7. Enter a name for the key.
8. (Optional) Enter and confirm a passphrase for the key.

9. Select how long you want the key to be valid: Lifetime, Days, or Years.
10. If you selected Lifetime in Step 9, jump to Step 11. If you selected Days or Years, in the new field that appears, specify exactly how many days or years the key should be valid.
11. (Optional) Enter any comments you want related to the SSH key you are uploading.

> **Note:** The Push automatically toggle is enabled by default.

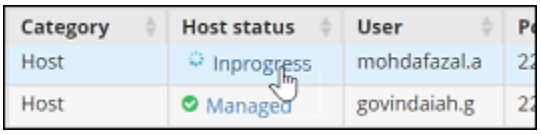
12. If you want to disable automatic pushing of the key to any new connectors that associated, click  to switch it to  .
    The Rotate automatically toggle is disabled by default.
13. If you want to enable automatic rotation of the SSH key for security compliance reasons, click  to switch it to  .
14. If you enable this feature, in the TTL (time-to-live) field that appears, specify the number of hours or days you want the key to be active before it gets rotated out.
15. Click **Upload** to upload the SSH key.

## Fetch Keys for an SSH Host

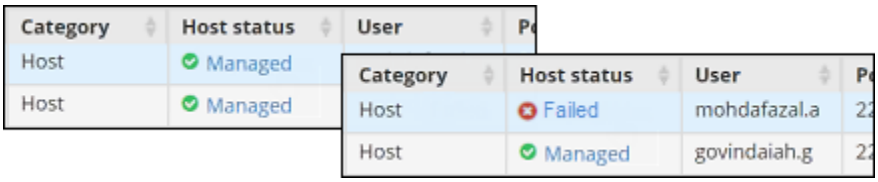
The number of keys that are discovered during the fetch operation outlined below depends on the type of account a user is logged in with. If a user logs in with their own personal account details, then the only keys fetched are those associated with the user's account. If the user logs in using the root credentials of an account, the fetch operation discovers all keys from all the user accounts in the device. If a user logs in as a superuser, called a Sudoer user, the fetch operation discovers all keys from all the user accounts in the device.

To fetch keys an SSH host:

1. Click  .
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the **Host** tab to open it.
4. Select the checkbox beside the SSH host that you want to fetch keys for.
5. Click  in the Command bar.
   The Host status column displays a status of In progress while the fetch operation is running.



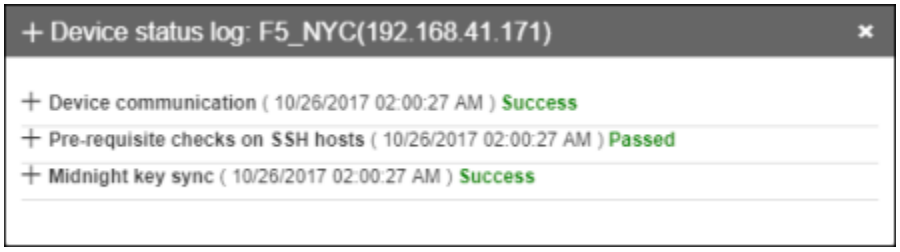

The status then changes to Managed if the fetch is successful or Failed or **Unresolved** if it is unsuccessful.




## View the Device Status Log for an SSH Host

To view the device status log for an SSH host:

1. Click ☰.
2. Navigate to **Inventory** > **SSH**.
   The SSH screen opens.
3. Click the **Host** tab.
4. If the host whose status log you want to view is not listed on the screen, run a search to locate it.
5. Click the link for the host in the Host status column.
   - If the host has a status of **Managed**, the log contains **Device communication**, **Prerequisite check**, and **Midnight key sync** status details.




   - If the host has a status of **Failed**, only the Device communication details appear.
   - If the status is In progress, the log shows whichever processes have completed or failed so far.

## Associate a Client Device with an SSH Key

To associate an SSH client device or group of devices with an SSH key:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key whose details you want to view is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the SSH key you want to associate a device with.
5. On the SSH key topology that opens, click on the left side of the key.
   You can choose between **Regular** and **Vault**.
   - By enabling the **Regular** option, you can enable only the key pair push to the end-device user account.
   - By enabling the **Vault** option, you have to choose the vault vendor for which the private key has to be pushed. If you select CyberArk, the private key will be pushed to the CyberArk user account and also to the end device user account.

   **Note:** When the regular connector type is selected, the push operation workflow will be triggered for the (client) end device user account only. When the Vault: CyberArk option is selected, then the workflow for private key push will be triggered for the end device user account. If this process is successful, the private key push to the CyberArk user account will be initiated by the same workflow.

   **Note:** You will have access to the following options only when the **Publish SSH private keys to CyberArk user account** option in **Settings > SSH > Cyberark Web Authentication** is enabled.

6. In the Host tab, select the server or host to be associated with the key.
7. To associate the host to the new or existing device(s), you can do the following:

   a. Search for and select the existing devices.

   b. If you want the new device to be associated, click .
      The device and the related SSH key will then be associated.

8. Click **Next** and on the Assign Users screen, select the users to which the host must be associated.
9. Click **Next** to view the **Summary**. On the Summary screen, review each of the users and devices you have selected and, if necessary, click the Remove User link beside the name of any user who you no longer want to associate with the key. Click the X icon beside any device that you no longer want to include.

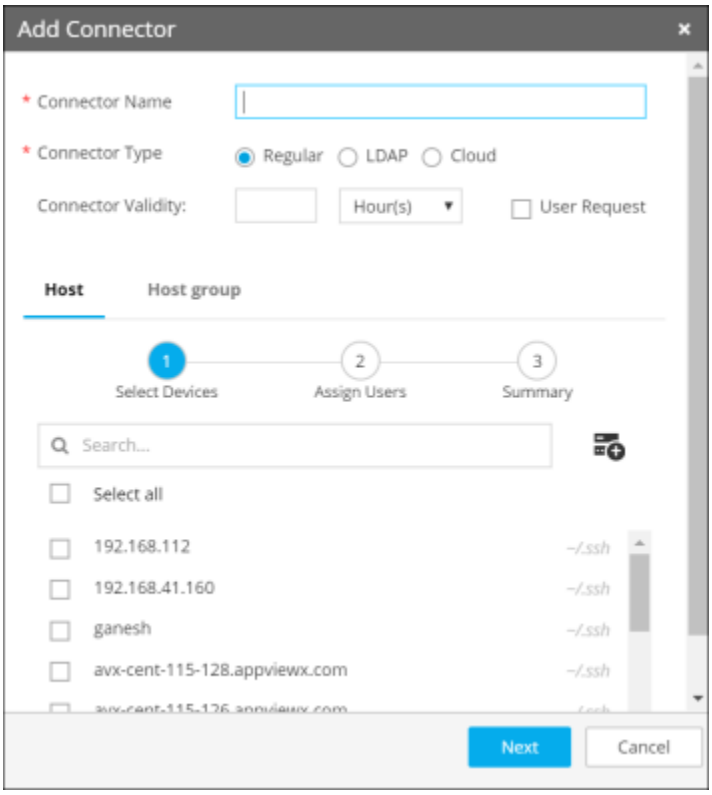
10. Click the Host group tab, then select the checkbox beside each host group you want to associate with the key.
11. Click Add to finish associating the client host with the key.
12. If the SSH key setting for Push automatically is disabled, you must then push the key to the new device manually. You can do this by right-clicking the device and selecting Push to device from the dropdown menu that appears.

## Associate a Server Device with an SSH Key

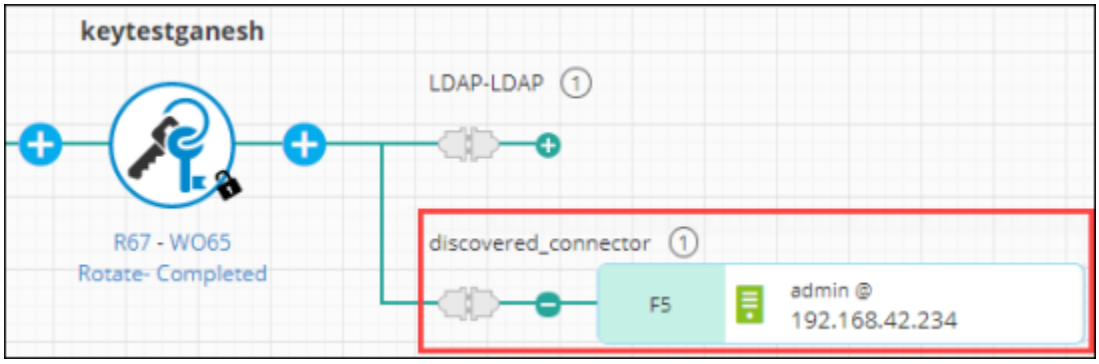
**Note:** For LDAP, GCP, and AWS connector types, you cannot associate more than one user account to the existing key.For the Cloud vendor, the list of hosts displayed is based on the account you selected.This field is used to grant specific users access to a key for a limited time. For complete details on how to use this feature, refer to the Set Up Privileged Access Management for an SSH Key section of this guide.The validity time frame here relates only to the association between the device and the SSH key. The SSH key has its internal validity timeframe that determines how long it is valid in the system, irrespective of which devices it is associated with.

To associate a server device or group of devices with an SSH key:

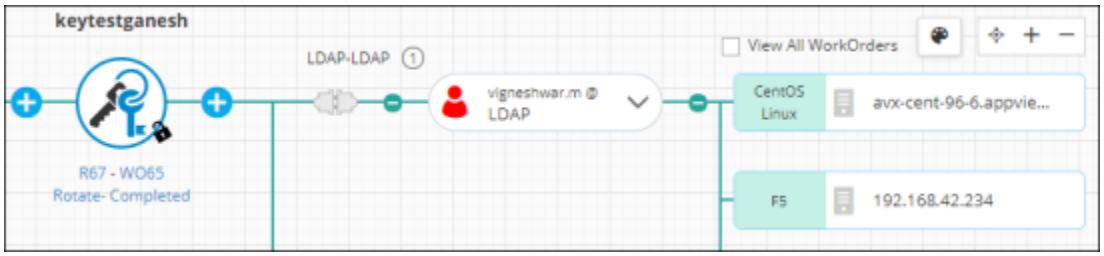
1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key whose details you want to view is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the SSH key you want to associate a device with.
5. On the SSH key topology that opens, click on the right side of the key.
6. The Add connector panel that pops-up up is where you will create the connector and determine which device or group of devices will be associated with the SSH key as well as which users will be associated with the devices. When you finish adding the connector, the SSH key is then pushed to each user you selected.



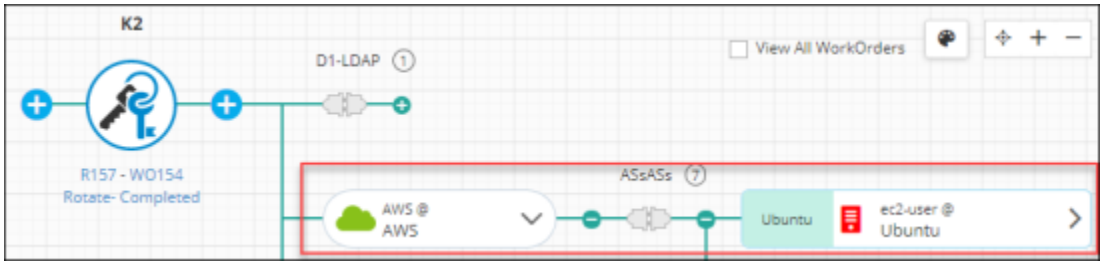

7. Enter a name for the connector you are creating.
8. Select one of the following types of connectors:
   - **Regular** - Associates and manages an SSH key in the servers. The holistic view displays the direct connection between the host and the connector.




   - **LDAP** - Associates and manages an SSH key in Active Directory (AD) user-profiles and servers. The holistic view displays the AD user profile that is associated with the connector, on the left side, and to the server, on the right side.



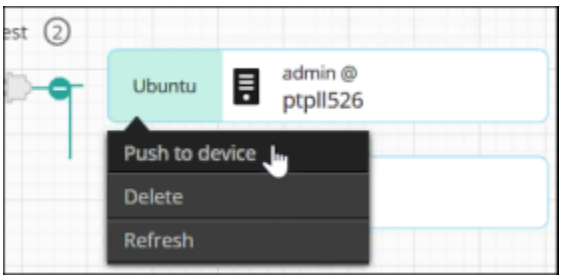

- **Cloud** - Associates and manages an SSH key in the cloud vendor SSH key inventory and instances (host). The holistic view is based on the cloud vendor business rules.




9. Leave the **User Request** checkbox unselected.
10. In the Connector validity field, select the length of time you want the public key to be associated with the server device or devices. After the time runs out, the connector will no longer be valid and the public key would be deleted from the servers.
11. From the **Cloud Vendor** dropdown menu, select the name of your cloud vendor (this is only for the connector type **Cloud**).
12. From the **Account Name** dropdown menu, select the account that was created in the device inventory (this is only for the connector type **Cloud**). For more details on how to add a cloud account, refer to the Add a Device section of this guide.
13. In the Host region, select the server or host to be associated with the key.
14. To associate the host to the new or existing device(s), you can do the following:
    a. Search for and select the existing devices
    b. If you want the new device to be associated, click  . The device and the related SSH key will then be associated.
15. Click **Next** and on the **Assign Users** screen, select the users to which the host must be associated.
16. Click **Next** to view the **Summary**.
17. On the Summary screen, review each of the users and devices you have selected and, if necessary, click the Remove User link beside the name of any user who you no longer want to associate with the key.
18. Click the X icon beside any device that you no longer want to include.
19. Click **Next**.

20. Click the **Host Group** tab, then select the checkbox beside each host group you want to associate with the key.
21. Click **Add** to finish associating the connector to the key.
22. If the SSH key setting for Push automatically is disabled, you must then push the public key to the new device manually. You can do this by right-clicking the device and selecting Push to device from the dropdown menu that appears.

> **Note:** For more details, refer to the Push an SSH key to the Device section of this guide.




## Modify an SSH Key Connector

To edit an SSH key connector:

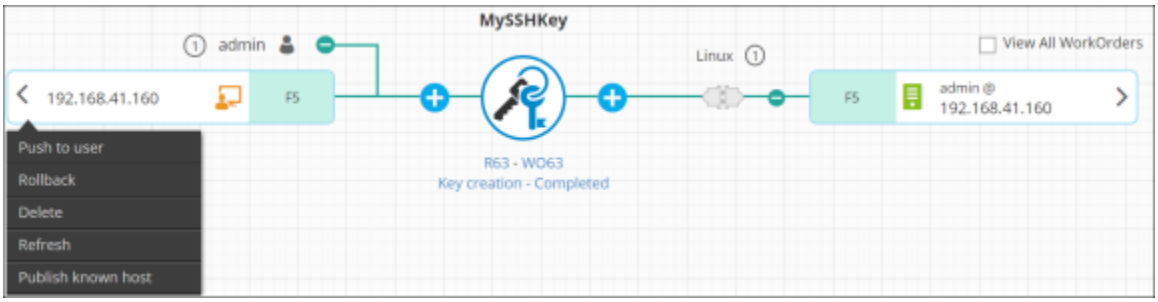
1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key whose connector you want to modify is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the SSH key.
5. On the SSH key topology that opens, right-click the connector that you want to modify and select **Modify** from the drop-down menu.
6. On the Add connector panel that appears, change whatever details you want.
7. When you have finished, click **Update**.

## Update a Known Host File

To update or publish a known host file (for a specific user) to the client by reading it from the server:

1. Create an SSH Key.
2. Associate a Client Device with an SSH Key and Associate a Server Device with an SSH Key.

3. If you enabled the automatic push option, the known host file with the work order on the client device is published immediately. Steps 3 to 9 below explain what to do if the automatic push option was not enabled or if publishing of the host file fails. If the key is pushed to the client and server devices successfully for a particular user, then right-click the client device.




The public known host appears only when the color code of the client device is set to 'orange'. This indicates that the host is not updated. For more details, refer to the View the Different Statuses and States for an SSH Key and Hostsection of this guide. From the dropdown menu that appears, click the **Publish known host** option.

4. Right-click the host again and click **Approve** from the dropdown menu that appears.

> **Note:** When auto push is disabled for a key, the system will not update the known host in client devices. You can update the known host file only using workflows.

5. On the Approve popup screen that appears, enter any comments you have about the creation, then click Yes.
6. Right-click the host and click **Implement** from the dropdown menu that appears.
7. On the Implement screen that pops up, enter any comments about the implementation, then click Yes.
8. Click in the top corner of the holistic view to refresh the screen until the host shows a status of Known host - Completed.

## Set Up Privileged Access Management for an SSH Host

If you want to grant specific users access to an SSH host for a limited amount of time, you can set up Privileged Access Management (PAM) for the key.

To set up PAM:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. Click the **Host** tab to open it.

3. If the SSH host you want to set up PAM for is not visible on the screen, use the Search field to locate it.
4. Select the host(s) for which you want to add the PAM.
5. Click  in the command bar.
   The **Timebound Access** panel containing five steps pops up.
6. On the **Access Duration** screen, click inside the From fields, specify the date and time during which you want the user to be granted access to the SSH host. The time you select is the exact time that the user will be granted access to the device (after approval of the corresponding work order).
7. In the **To** field, specify the time when you want to end the user's access to the device. The time you select is the exact time the host will be automatically deleted from the device with the help of the work order.
8. Click **Next**.
   The **Assign Users** screen appears.
9. Select the users to whom you want to provide access to the critical devices for a limited time frame.
10. Click **Next**.
    The **Select Keys** screen appears.
11. Select the appropriate SSH keys of the user to be used in initiating the SSH sessions during the requested time frame.
12. Click **Next**, the **Client Devices** screen appears.
13. (Optional) Choose the source and destination (client device to push the private key pair) for the selected server devices.
14. Click **Next**, the **Summary** screen appears.
15. Click **Done** to initiate the request or you can click any particular step to modify your choices if required. After submitting, the device associations can be viewed in the SSH key inventory and the respective key holistic view.

## Delete an SSH Key from a Connector

In order to delete your own SSH keys from a connector, you must be logged in with a role that has been granted the Host level action > Delete > User owned keys permission in the Account module. If you want to delete other user's SSH keys, you must have been granted the Host level action > Delete > Other user keys permission.

A device is associated with the SSH key using three types of connectors, namely, Regular, LDAP, and Cloud. The procedure to delete an SSH key from LDAP or Cloud connectors is similar to the procedure explained below.

To delete an SSH key from a connector:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to delete is not visible on the screen, use the Search field to locate it.

> **Note:** For information on how to delete an SSH key from the AppViewX database, refer to Delete an SSH Key from the Database.

4. Click the link in the Key name column for the key you want to delete. The holistic view appears, with the SSH key displayed.
5. Right-click on the connector and select Delete from the menu that appears.
   The Delete screen that pops up varies according to the connector type.
6. Select the following checkboxes and then click **Yes**, to delete an SSH key.
   - LDAP - **Delete from LDAP directory server** and **Disassociate LDAP directory from key (holistic view)**
   - Cloud - **Delete key from device** and **Disassociate host from key (holistic view)**
7. On the screen that pops up, click **Yes** to confirm that you want to delete the key.
   If the key policy does not require work order approval, then the key deletion process is complete. If the key policy does require work order approval, the process continues through the following steps.
8. On the holistic view screen, the key status changes to In Progress (Key Deletion - Approval level 1).
9. Right-click the key and select Approve from the dropdown menu that appears.
10. On the Approve popup screen that appears, enter any comments you have about the deletion, then click **Yes**.

> **Note:** If the key is already pushed to the connector, you can only disassociate the host from the key after the key has been successfully deleted from the connector. If the deletion fails, the disassociation cannot take place.

11. Click in the holistic view to refresh the screen until the key shows a status of In Progress (Key Deletion - Awaiting implementation).
12. Right-click the key and select Implement from the dropdown menu that appears.
13. On the Implement screen that pops up, enter any comments about the implementation, then click **Yes**.
14. Click in the holistic view to refresh the screen until the key shows a status of Key deletion - Completed.
    At this point, the process is complete: the key has been deleted from the connector. However, it still exists in the database and can be viewed in the list of SSH keys on the SSH: Key screen.

## Delete an SSH Key from a Device

In order to delete your own SSH keys from a device, you must be logged in with a role that has been granted the Host level action > Delete > User owned keys permission in the Account module. If you want to delete other user's SSH keys, you must have been granted the Host level action > Delete > Other user keys permission.

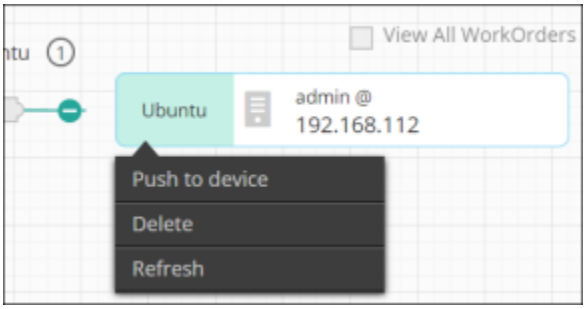
A device is associated with the SSH key using three types of connectors, namely, Regular, LDAP, and Cloud. The procedure to delete an SSH key from the device having one of those connectors is similar to the procedure explained below.

To delete an SSH key from a device:

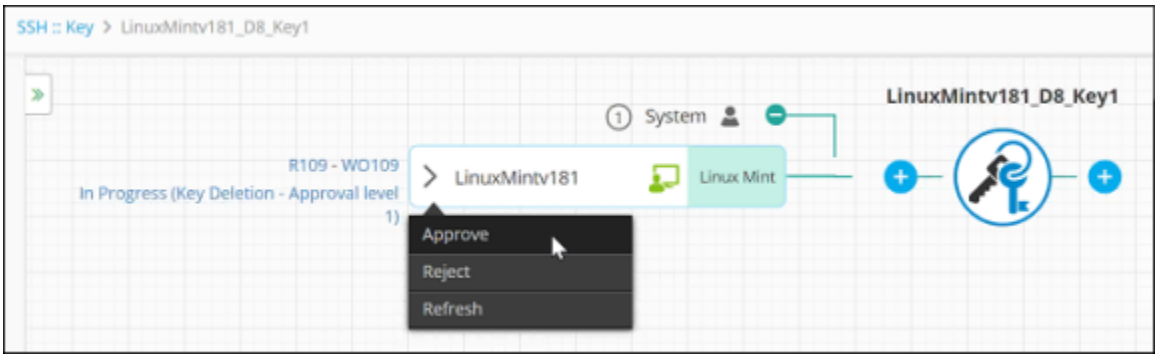
1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to delete is not visible on the screen, use the Search field to locate it.

> **Note:** For information on how to delete an SSH key from the AppViewX database, refer to Delete an SSH Key from the Database.

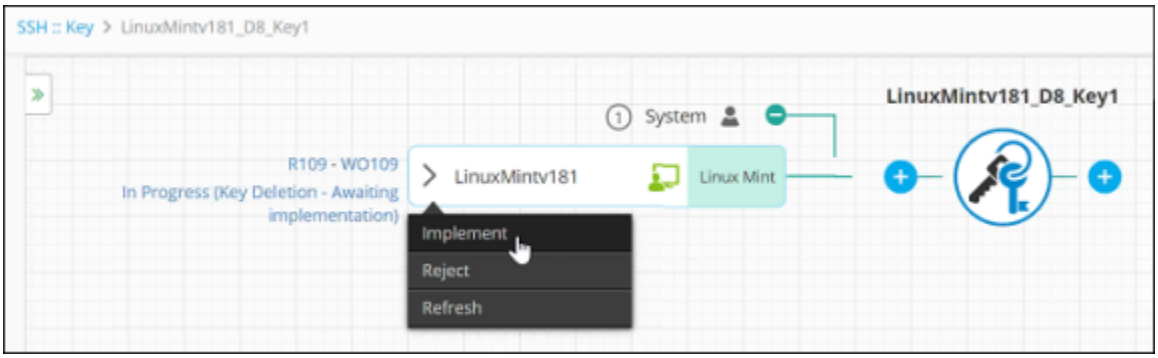
4. Click the link in the Key name column for the key you want to delete.
   The holistic view appears, with the SSH key displayed.
5. Right-click on the device and select Delete from the menu that appears.



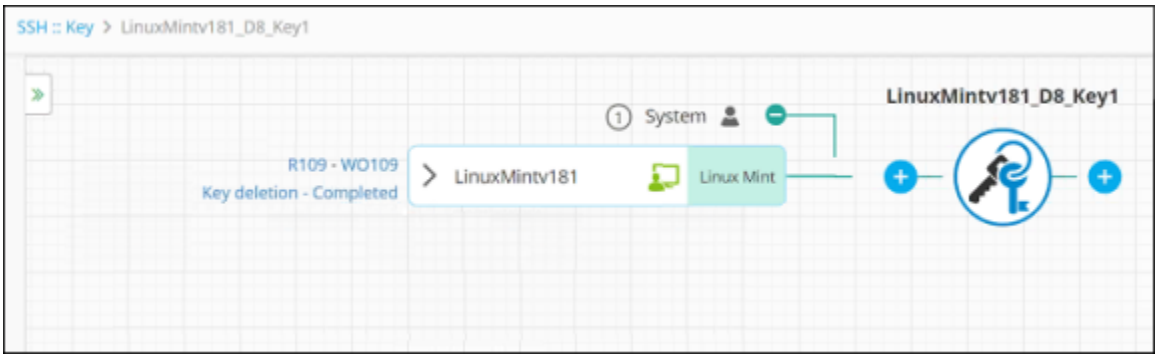

   The Delete screen that pops up varies according to the connector type.
6. Select the following checkboxes and then click **Yes**, to delete an SSH key.
   - Regular - Delete key from device and Disassociate host from key (holistic view)
   - LDAP - **Delete key from device** and **Disassociate host from LDAP directory (holistic view)**
   - Cloud (Azure, GCP, and AWS vendors) - **Delete key from device** and **Disassociate host from key (holistic view)**.




7. On the screen that pops up, click **Yes** to confirm that you want to delete the key.
   If the key policy does not require work order approval, then the key deletion process is complete. If the key policy does require work order approval, the process continues through the following steps. On the holistic view screen, the key status changes to In Progress (Key Deletion - Approval level 1).
8. Right-click the key and select Approve from the dropdown menu that appears.
9. On the Approve popup screen that appears, enter any comments you have about the deletion, then click **Yes**.
10. Click  in the holistic view to refresh the screen until the key shows a status of In Progress (Key Deletion - Awaiting implementation).
11. Right-click the key and select Implement from the dropdown menu that appears.




12. On the Implement screen that pops up, enter any comments about the implementation, then click **Yes**.
13. Click  in the holistic view to refresh the screen until the key shows a status of Key deletion - Completed.




At this point, the process is complete: the key has been deleted from the device. However, it still exists in the database and can be viewed in the list of SSH keys on the SSH: Key screen.

## Delete an SSH Key from the Database

To delete an SSH key from the AppViewX database, you must be logged in with a role that has been granted the Key level action > Delete (from AppViewX database) permission in the Account module.

**Note:** For information on how to delete an SSH key from a device, but keep it in the database, refer to Delete an SSH Key from a Device.

The steps involved in deleting an SSH key from the database differ depending on whether or not the key is associated with a key policy that requires work order approval and implementation of all actions initiated on the key. The instructions below cover both of these possibilities.

## No Work Order Required by the SSH Policy

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to delete is not visible on the screen, use the Search field to locate it.
4. Select the checkbox beside the SSH key you want to delete.
5. Click in the Command bar.
6. On the confirmation screen that appears, click **Yes**.
   The key is then removed from the list and deleted from the AppViewX system.

## Work Order Required by the SSH Policy

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to delete is not visible on the screen, use the Search field to locate it.
4. Select the checkbox beside the SSH key you want to delete.
5. Click in the Command bar.
6. On the confirmation screen that appears, click **Yes**.
   The SSH key appears in a holistic view with a status of In Progress (Key Deletion - Approval level 1).
7. Right-click the key and select Approve from the dropdown menu that appears.


8. On the Approve popup screen that appears, enter any comments you have about the deletion, then click **Yes**.
9. Click in the holistic view to refresh the screen until the key shows a status of In Progress (Key Deletion - Awaiting implementation).
10. Right-click the key and select Implement from the dropdown menu that appears.

11. On the Implement screen that pops up, enter any comments about the implementation, then click Yes.
    The SSH: Key screen then reopens.
12. Click  in the Command bar to refresh the contents of the page. The SSH key no longer appears in the database.

## Delete an SSH Host

To delete an SSH host:

1. Click  and select **Inventory** > **SSH**.
   The SSH screen opens.
2. Click the **Host** tab to open it.
3. If the SSH host you want to delete is not visible on the screen, use the Search field to locate it.
4. Select the checkbox beside the SSH host you want to delete.
5. Click  in the Command bar.
6. On the confirmation screen that appears, click **Yes**.
   The host is then removed from the list and deleted from the AppViewX system.

## Delete an SSH Policy

To delete an SSH policy:

1. Click  and select **Inventory** > **SSH**.
   The SSH screen opens.
2. Click the Policy tab to open it.
3. If the SSH policy you want to delete is not visible on the screen, use the Search field to locate it.
4. Select the checkbox beside the SSH policy you want to delete.
5. Click  in the Command bar.
6. On the confirmation screen that appears, click **Yes**.
   The policy is then removed from the list and deleted from the AppViewX system.

## Change the Status of an SSH Key

Before changing the status of an SSH key, you should carefully consider and plan for the impact the change might have on existing work orders.

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Server tab is not displayed, click to open it.
3. In the server list, select the checkbox beside the SSH key whose status you want to change.
4. Click in the Command bar.
5. On the Change status pop-up screen that appears, click the Change status to dropdown list and select either Managed or Monitored.
6. (Recommended) In the Comments field, enter the reason why you are changing the status.
7. Click **Yes** to change the status.

## Assign or Unassign a Group to an SSH Key

### Assign a Group

To assign or unassign a group to an SSH key:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. In the list of SSH keys, select the checkbox beside the key that you want to assign a group to.
4. In the Command bar, click
5. On the Assign group screen that appears, select the checkbox beside the group that you want to assign to the key.
6. Click the Assign button.

### Unassign a Group

To unassign a group from an SSH key:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. In the list of SSH keys, select the checkbox beside the key that you want to unassign a group from.
4. In the Command bar, click .

## Export an SSH Key

To export an SSH key:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. In the list of SSH keys, select the checkbox beside the key you want to export.
4. Click in the Command bar.
5. On the Export pop-up screen that appears, choose whether you want to export all columns of data for the key or just the columns that are currently visible on the Key tab.
6. Choose whether to save the exported certificate as a CSV or an XLS file.
7. Click **Export**.
8. Select the location where you want to export the file, then click **Save** to complete the export.

## Export an SSH Host

To export an SSH host:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. Click the Host tab to open it.
3. In the list of SSH hosts, select the checkbox beside the host you want to export.
4. Click in the Command bar.
5. On the Export pop-up screen that appears, choose whether you want to export all columns of data for the SSH host or just the columns that are currently visible on the Host tab.
6. Choose whether to save the exported host as a CSV or an XLS file.
7. Click **Export**.
8. Select the location where you want to export the file, then click **Save** to complete the export.

## Download a Public SSH Key

You can download a public SSH key from two locations within AppViewX application: from the SSH Key tab and from the holistic view that contains the SSH key.

## Download from the SSH Key Tab

To download a public SSH key from the Key tab, complete the following steps:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Select the check box beside the SSH key whose public key you want to download.
5. Click in the Command bar.
   The Download public key screen appears.
6. In the Format field, select one of the following options:
   - .txt(PKCS8)
   - .txt(RFC4716)
   - .txt(PEM) - This option is not available for DSA and ECDSA encryption.
7. Click OK to download the key.

## Download from a Holistic View

To download a public SSH key from a holistic view, complete the following steps:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the key.
   The holistic view appears, with the SSH key displayed.
5. Right-click on the SSH key and select Download public key from the menu that appears.
   The Download public key screen appears.
6. In the Format field, select one of the following options:
   - .txt(PKCS8)
   - .txt(RFC4716)
   - .txt(PEM) - This option is not available for DSA and ECDSA encryption.
7. Click OK to download the key.

## Download a Private SSH Key

You can download a private SSH key from two locations within AppViewX application: from the SSH Key tab and from the holistic view that contains the SSH key.

## Download from the SSH Key Tab

To download a private SSH key from the Key tab, complete the following steps:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Select the check box beside the SSH key whose private key you want to download.
5. Click in the Command bar.
   The Download private key screen appears.
6. If the select key has a passphrase, enter it in the Enter the passphrase field.
7. In the Format field, select one of the following options:
   - PEM (.pem) - Downloads the private SSH key in Privacy Enhanced Mail (.pem) format. This format is an Internet standard that provides for secure exchange of email through the use of a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity. This option is not available for ECDSA key encryption.
   - PTF (.txt) - Downloads the private SSH key in text file format (.txt).
   - PuTTY (.ppk) - Downloads the private SSH key in PuTTY Private Key Header (.ppk) file format.
8. Click OK to download the key.

> **Note:** To download a private SSH key in .ppk file format, ensure that the PuTTYgen version 0.70 is installed on the server.

## Download from a Holistic View

To download a private SSH key from a holistic view, complete the following steps:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. If the Key tab is not displayed, click to open it.
5. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
6. Click the link in the Key name column for the key.
   The holistic view appears, with the SSH key displayed.
7. Right-click on the SSH key and select Download private key from the menu that appears.

The Download private key screen appears.

8. If the select key has a passphrase, enter it in the Enter the passphrase field.
9. In the Format field, select one of the following options:

**Note:** To download a private SSH key in .ppk file format, ensure that the PuTTYgen version 0.70 is installed on the server.

   - PEM (.pem) - Downloads the private SSH key in Privacy Enhanced Mail (.pem) format. This format is an Internet standard that provides for secure exchange of email through the use of a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity. This option is not available for ECDSA key encryption.
   - PTF (.txt) - Downloads the private SSH key in text file format (.txt).
   - PuTTY (.ppk) - Downloads the private SSH key in PuTTY Private Key Header (.ppk) format
10. Click OK to download the key.

## Rollback an SSH key

Rollback option allows you to revert the action performed on the SSH key to an immediate previous state.

## From an SSH key

To perform a rollback action from the SSH key:

1. Click  and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the **Key name** column for the key you want to delete. The holistic view appears, with the SSH key displayed.
5. Right-click on the SSH key and select **Rollback** from the menu that appears.
6. On the Rollback screen that pops up, enter the passphrase that you had mentioned while generating the SSH key.
7. Enter any comments you have about the rollback action, then click **Yes**.
   If the key policy does not require work order approval, then the rollback process is complete.

## From a Client or Server device

To perform a rollback action from the client or server device:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the **Key name** column for the key you want to delete.
   The holistic view appears, with the SSH key displayed.
5. Right-click on the client or server device and select **Rollback** from the menu that appears.
6. On the **Rollback** screen that pops up, enter any comments you have about the rollback action, then click **Yes**.
   If the key policy does not require work order approval, then the rollback process is complete.

## From the Cloud inventory

To perform a rollback action from the cloud inventory:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the **Key name** column for the key you want to delete. The holistic view appears, with the SSH key displayed.
5. Right-click on the cloud inventory (of GCP and AWS connector types) and select **Rollback** from the menu that appears.
6. On the **Rollback** screen that pops up, enter any comments you have about the rollback action, then click **Yes**.
   If the key policy *does not* require work order approval, then the rollback process is complete.

## Work Order Required by the SSH Policy

If the key policy does require work order approval:

1. On the holistic view screen of the respective SSH Key, the status changes to In Progress (Rollback - Approval level 1).
2. Right-click the SSH key or the device and select Approve from the dropdown menu that appears.
3. On the Approve popup screen that appears, enter any comments you have about the deletion, then click Yes.
4. Click in the holistic view to refresh the screen until the key shows a status of In Progress (Rollback - Awaiting implementation).

5. Right-click the SSH key or the device and select Implement from the dropdown menu that appears.
6. On the Implement screen that pops up, enter any comments about the implementation, then click Yes.
7. Click  in the holistic view to refresh the screen until it shows a status of Rollback - Completed.
   At this point, the process is complete: the rollback action has been performed from the selected key or the device.

> **Note:** You might have to click  a few times to update the screen to see the status change

## Rotate an SSH Key

To rotate an SSH key, complete the following steps:

1. Click  and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the key. The holistic view appears, with the SSH key displayed.
5. Right-click on the SSH key and select **Rotate** from the menu that appears.
6. If the key policy does not require work order approval, then the key deletion process is complete.
7. If the key policy does require work order approval, the process continues through the following steps.
8. On the holistic view screen, the key status changes to In Progress (Approval level 1).
9. Right-click the key and select Approve from the dropdown menu that appears.
10. On the Approve popup screen that appears, enter any comments you have about the approval, then click **Yes**.
11. Click  in the holistic view to refresh the screen until the key shows a status of In Progress (Awaiting implementation).
12. Right-click the key and select Implement from the dropdown menu that appears.
13. On the Implement screen that pops up, enter any comments about the implementation, then click Yes.
14. Click  in the holistic view to refresh the screen until the key shows a status of Rotate - Completed.
15. At this point, the process is complete: the key has been rotated.

## Renew an SSH Key

To renew an SSH key:

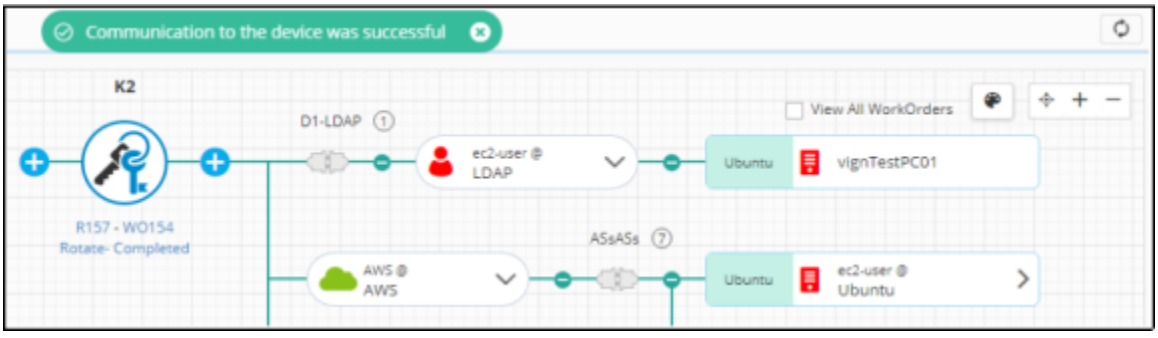
1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the key.
   The holistic view appears, with the SSH key displayed.
5. Right-click on the SSH key and select Renew from the menu that appears.

## Refresh the Component

The Refresh option is used to communicate and fetch the latest data from the LDAP directory, AWS inventory, Client device, or Server device.

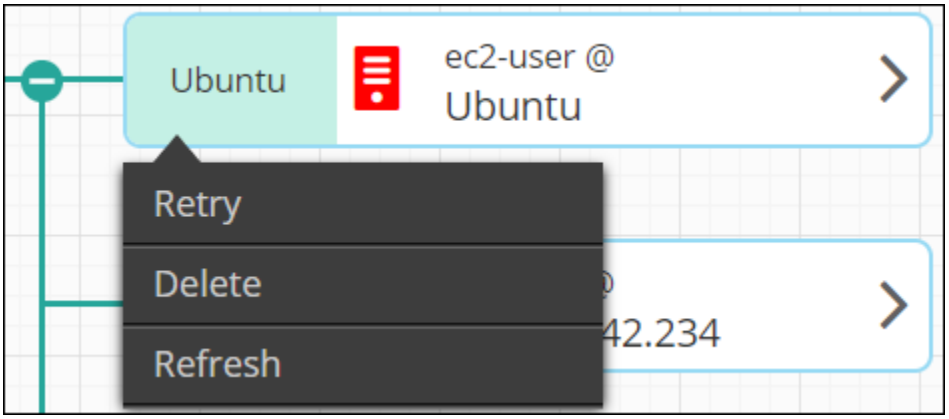
To refresh the data:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. If the Key tab is not displayed, click to open it.
3. If the SSH key you want to access is not visible on the screen, use the Search field to locate it.
4. Click the link in the Key name column for the key.
   The holistic view appears, with the SSH key displayed.
5. Right-click on the respective component (such as LDAP directory, AWS inventory, GCP inventory, Azure account connector, Client device, and Server device) as needed and select Refresh from the menu that appears.
   If the component is updated successfully, the following message is displayed: **Communication to the device was successful**.



## Retry a Failed Workorder

If the work order fails while performing an action on the SSH key, connector, or device, the respective component will be highlighted in red. You can right-click the component, and then click **Retry** to trigger the action again.




## Monitor SSH Sessions

To view the status of the SSH session at a given point of time:

1. Click and select **Inventory** > **SSH**.
   The SSH screen opens.
2. Click the **Host** tab to open it.
3. If the SSH host whose SSH sessions you want to view is not visible on the screen, use the Search field to locate it.
4. Select the host for which you want to view the SSH sessions.
5. Click in the command bar. A new screen displaying the active sessions to the client devices.
6. Select the sessions that are not required and click **Terminate**.

# Group Tasks

- Overview
- Add an ADC Group
- Create a Certificate Group
- Create an SSH Group
- View All Keys Associated with an SSH Group
- Modify an ADC Group

- Modify a Certificate Group
- Modify an SSH Group
- Delete a Certificate Group
- Add a Command Profile Group

## Overview

The Group screen within the Inventory module allows you to perform the following tasks:

- Add an ADC group
- Create a certificate group
- Create an SSH group
- Modify an ADC group
- Modify a certificate group
- Modify an SSH group
- Delete an ADC, certificate, or SSH group
- Delete a certificate group

## Add an ADC Group

To add an ADC group to AppViewX:

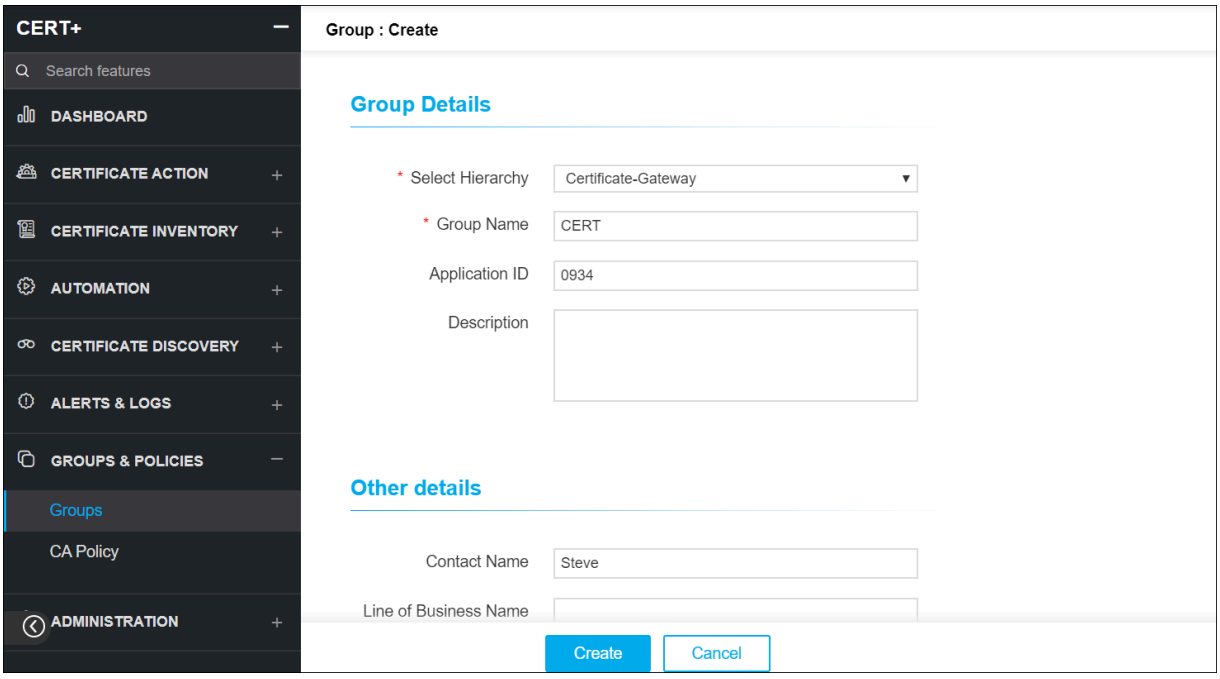
1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. If the ADC tab is not displayed by default, click to open it.
3. Click + in the Command bar.
4. On the Add screen that appears, enter a name for the new group. (Recommended) Enter a description of the group to help users identify it.
5. In the Device selection field, click » beside each device you want to include in the group.
6. When you have finished assigning devices to the group, click Save to add it 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.

## Create a Certificate Group

To create a certificate group in AppViewX:

1. Click  and select **Inventory** > **Groups&Policies**.
2. Under **Groups & Policies**, click **Groups**.
3. On the Groups list view page, click **+ Create** on the top-right.
4. On the create details page, under the **Group Details** section**,** select a hierarchy.
5. Enter a name for the new group.
6. Enter the ID of the application the certificate group is to be associated with.
7. (Recommended) Enter a description of the certificate group to help users identify it.
8. Under **Other Details** section, provide any or all of the following details about the certificate group:
   - Contact name
   - LOB name - Line-of-business (LOB) manager responsible for reviewing access privileges for all users
   - Contact's email address
   - Environment name
   - Contact's phone number
   - Inventory number
   - Cost center/Hierarchy under which the certificate group appears
9. Click **Create** to add the certificate group to the system.




**Note:** You can also create a certificate group for **Server**, **Client**, and **Device** certificates by clicking from the respective tabs under **Certificate** inventory.

## Create an SSH Group

To create an SSH group in AppViewX:

1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. Click the SSH tab at the top of the screen.
3. Click in the Command bar.
4. On the Create screen that appears, enter a name for the new group.
5. (Recommended) Enter a description of the SSH group to help users identify it.
6. Select the type of SSH group you want to create: Key or Host.
7. If you selected Key in Step 7, jump to Step 9. If you selected Host, in the Entity selection field that appears, select the checkboxes beside each of the entities you want to include in the SSH group, then click the Add as Regex button.
8. Click Create to add the SSH group to the system.

## View All Keys Associated with an SSH Group

To create an SSH group in AppViewX:

1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. Click the SSH tab at the top of the screen.
3. If the SSH group whose keys you want to see is not displayed on the screen, run a search for it.
4. In the Count column, click the link for the SSH group.
   A popup screen appears, listing all of the keys associated with the SSH group.


## Modify an ADC Group

To modify an ADC group to AppViewX:

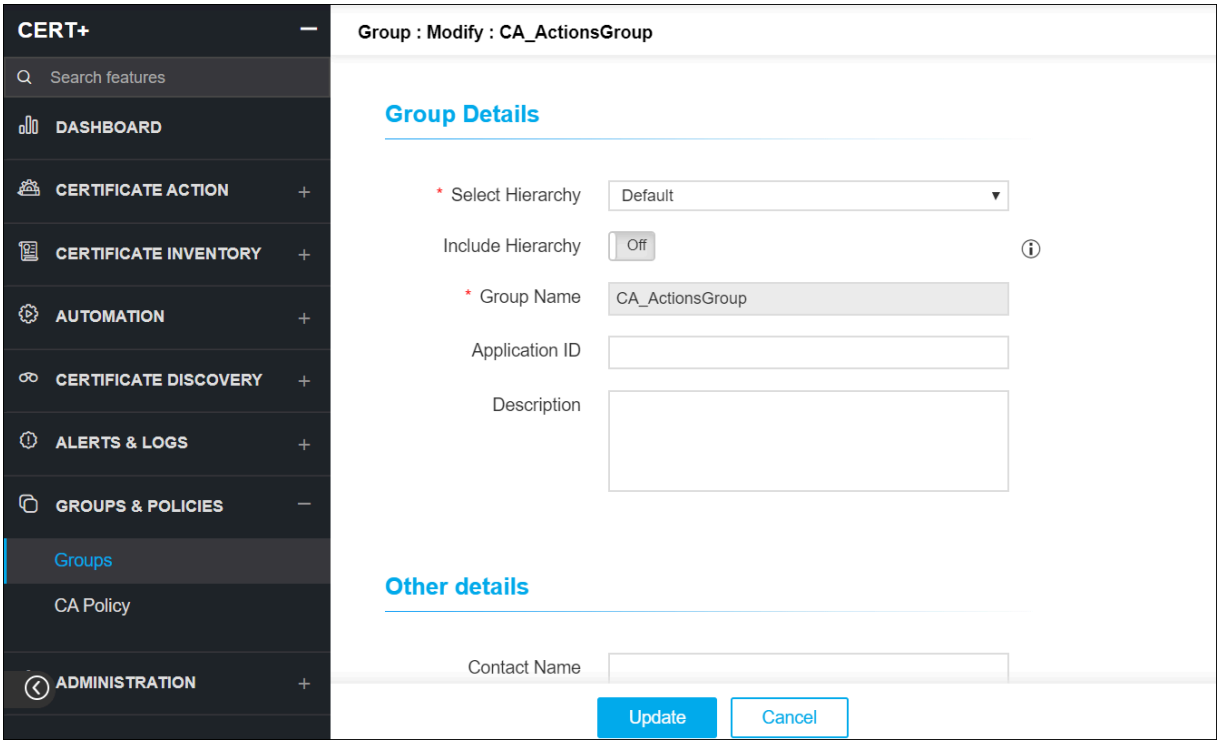
1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. If the ADC tab is not displayed by default, click to open it.
3. If the ADC group whose details you want to modify is not displayed on the screen, use the search field to locate it.
4. Select the checkbox beside the name of the ADC group.
5. Click in the Command bar.
6. On the Modify screen that appears, make whatever changes you want to the content.
7. Click **Update** to save your edits.

## Modify a Certificate Group

To modify a certificate group to AppViewX:

1. Click and select **Inventory** > **Group&Policies**.
2. Under **Groups & Policies**, click **Groups**.
3. On the Group list view page, clickon the **Name** of the group you want to modify.
4. On the Modify details page, make necessary changes.

5. Click **Update** to save the changes.




## Modify an SSH Group

To modify an SSH group to AppViewX, complete the following steps:

1. Click .
2. Navigate to **Inventory** > **Group**.
   The Group screen opens.
3. Click the SSH tab at the top of the screen.
4. If the SSH group whose details you want to modify is not displayed on the screen, use the search field to locate it.
5. Select the check box beside the name of the SSH group.
6. Click in the Command bar.
7. On the Modify screen that appears, make whatever changes you want to the content.
8. Click Update to save your edits.

## Delete a Certificate Group

Although the deletion of ADC, certificate, SSH, and Command profile groups is carried out on separate tabs within the Group screen, the process is identical for each.

To delete an ADC, certificate, SSH, or command profile group from the AppViewX system:

1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. Click the tab that corresponds to the type of group you want to delete: ADC, Certificate, SSH, or **Command profile**.
3. Select the checkbox beside the group you want to delete.
4. Click in the Command bar.
5. On the confirmation screen that pops up asking you if you are sure you want to proceed, click Yes.
   The group is then removed from the AppViewX system.

## Add a Command Profile Group

To add a command profile group to AppViewX:

1. Click and select **Inventory** > **Group**.
   The Group screen opens.
2. If the Command profile tab is not displayed by default, click to open it.
3. Click + in the Command bar.
4. On the Add screen that appears, in the **Command details** section, enter a name for the new command.
5. (Recommended) Enter a description of the group to help users identify it.
6. In the **Conditions** section, click +.
7. In the **Conditions** window that appears, complete the following steps:

   a. From the Command type dropdown, select one of the following options:
   - **Exact** - The entire line of command with which the commands to be executed must match completely.
   - **Contains** - The line of command which must be a part of the commands to be executed.

b. Enter the command that you want to use for validation.

c. When you have finished adding conditions to the group, click Add to save it to the system. The condition that has been created will be displayed in the table at the bottom. You can modify and remove the condition by clicking  and  .

8. Click **Add**.

# Backup and Restore Tasks



## Backup and Restore Tasks

The Backup and restore screen within the Inventory module allows you to perform the following tasks:

- Create a device backup group
- Edit the details of a backup group
- Delete a backup group

- Delete the backup and restore history for a device backup group
- Schedule a device backup
- View the backup schedule for a device
- Back up a device immediately
- View the backup history of a device
- Download the backup history of a device
- Restore a device or object
- Compare the backups of two devices
- Compare multiple configurations of an object
- Edit the settings of the Backup screen

## 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, complete the following steps:

1. Click  and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device type that you are creating a backup group for.
4. For **ADC**, in the **Backup** tab, you will have the list of user-defined backup groups along with the default group. In the default group, you can find the backup of the devices that are not a part of any user-defined backup group(s). The device backups that are generated in the control center will also fall under the default group.

   
   **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.

5. Click  on the top right.
   On the Create screen that opens, the Device type is displayed by default depending on the sub-tab you selected in step 4.
6. Enter a name for the backup group.

7. (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.
8. (Only applicable for ADC) Select the **Device** or **Device Group** radio button based on how you want to define the device and iHealth report backup.
9. In the Available devices field, click » beside each device whose backups and restores you want to include in the group.
10. 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.
11. In the Email configuration field, enter the email addresses, separated by commas, of all users who should be sent a copy of the backup.
12. (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."
13. Click **Save**.

    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.

## Edit the Details of a Device Backup Group

To edit the details of a device backup group, complete the following steps:

1. Click  and select **Inventory** > **Backup & Restore**.

   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on what you want to modify.
4. In the list of backup groups on the screen, click  for the device backup group you want to modify.
5. On the Modify screen that opens, make whatever changes you want to the fields.

    **Note:** Note that the Device Type field cannot be edited after the group is created.

6. Click **Save**.

## Delete a Device Backup Group

Deleting a device backup group is different than deleting *the records* for a group. If you delete the records for a group, the group remains in the system. If you delete a group, its name is removed from the system, but the records remain.

To remove a device backup group from the AppViewX system, complete the following steps:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on what you want to delete.
4. In the list of backup groups on the screen, click for the device backup group you want to delete.
5. On the popup screen that appears, you will have an option to enable **Retain the generated backups**. (This option will be enabled by default).
6. Click Yes to confirm that you want to delete the device backup group.
7. The device backup group is removed from the AppViewX system.
   - If the device(s) falls under any other user-defined group, the backup will be retained in the respective backup group.
   - If the device(s) doesn't fall under any user-defined group, the backup will be retained in the default backup group. If you want to permanently delete the backup group along with devices, then you can uncheck the **Retain the generated backups** option in the popup screen.

> **Note:** For details on how to delete all backup and restore records for a device within a device group, refer to Delete the Backup and Restore History for a Device.

## Delete the Backup and Restore History for a Device

Deleting all backups for a device within a device backup group is different than deleting the group, itself. If you delete the records for a particular device, the records for other devices in the group remain untouched. If you delete a device backup group, the group name no longer exists, but the records remain in the system.

To delete all backups for a device in a device backup group from the AppViewX system, complete the following steps:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device back up and restore history you want to delete.
4. In the list of backup groups on the screen, click for the device backup group whose backup and restore history you want to delete.
5. In the table that appears, click the **Device Name** link for the device whose history you want to delete.
6. On the Archive details screen that appears, click the **Delete** button.
7. On the popup screen that appears, click **Yes** to confirm that you want to delete the backup and restore history for the device group.

## Schedule a Device Backup

To schedule a device backup:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**,**Proxy**,or **Firewall**, depending on what you want to back up.
4. Click in the Command bar.
5. On the Create screen that opens, enter a name for the backup you are about to schedule.
6. (Optional) Enter a description of the backup.
7. In the Available devices field, click » beside each device you want to add to include in the backup.
8. Select the Scheduler radio button.
9. Depending on how often you want to schedule a backup, select the Daily, Weekly, Monthly, or Yearly radio button.
10. Type the starting date of the backup or click and select the date from the popup screen that appears.
11. Type the starting time for the backup or click and select a start time using the sliding bars for Hour and Minute. When you are finished, click Done to close the popup screen.
12. (Optional) If you want certain users to receive the backup automatically as an email attachment, enter their email addresses 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."
13. 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.

**Note:** 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 and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**,**Proxy**,or **Firewall**, depending on what you want to view.
4. In the list of backup groups on the screen, hover your mouse over for the device whose backup schedule you want to view.
   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 f5 device that appears in the image above.

## Back Up a Device Immediately

There are two ways to back up a device immediately through the **Edit** screen and **Archive Details** screen. The first method turns off all other scheduled backups that most users would not want to do. The following instructions explain to back up a device immediately through the **Archive Details** screen.

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**,Proxy,or **Firewall**, depending on what you want to back up.
4. In the list of backup groups on the screen, click for the device you want to back up immediately.
5. Click the Device name link in the table that appears.
6. On the Archive details screen that appears, click **Backup Now**.

## View the Backup and Restore History for a Device

To view a list of all backups and restores for a device within a device backup group:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device back up and restore history you want to view.
4. In the list of backup groups on the screen, click for the device backup group that contains the device whose history you want to view.
5. In the table that appears, click the Device name link for the device whose history you want to view.
   The Archive details screen appears, listing all of the back-ups and restore events for the device.
   (Optional) Use the search field and calendar filter to locate specific backup or restore events based on filename, file path, or date range.

## Download the Backup and Restore History for a Device

To download a list of all backups and restores for a device within a device backup group, complete the following steps:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.

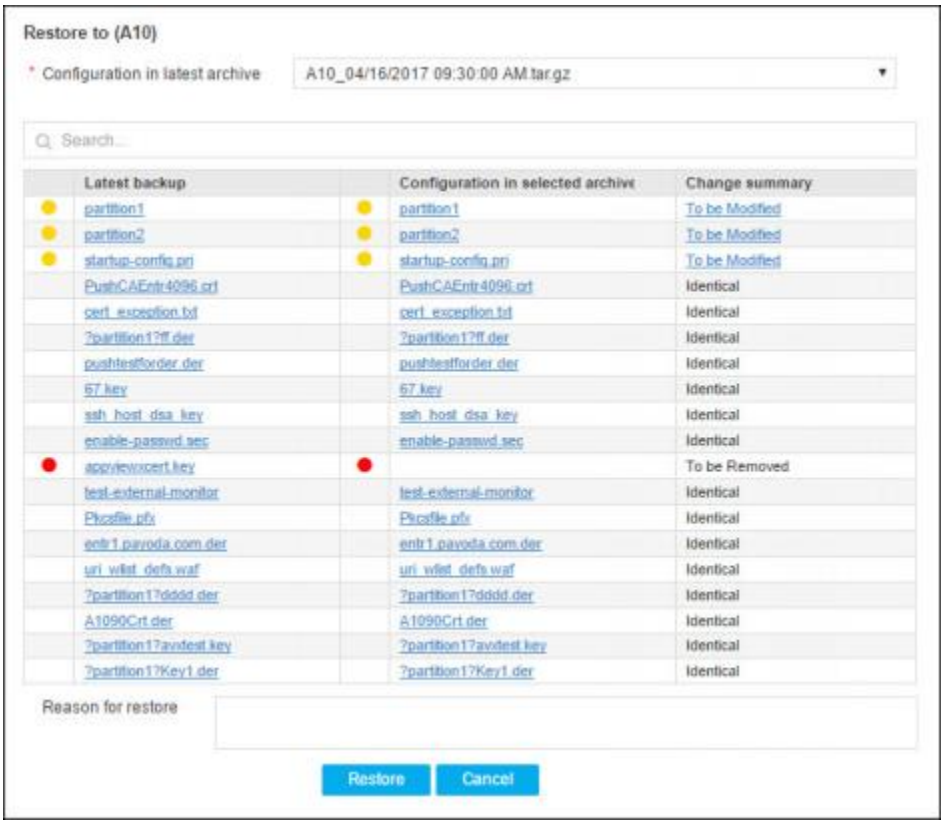
2. and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
3. If the Backup tab is not displayed by default, click to open it.
4. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device backup and restore history you want to view.
5. In the list of backup groups on the screen, click ➕ for the device backup group that contains the device whose history you want to download.
6. 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 backup and restore events for the device.
7. 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 for each result you want to download.

## Restore a Device or Object

To restore a device or object, complete the following steps:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device type that you want to restore.
3. Click the **Restore** tab.
4. (Only applicable for ADC) On the Restore screen that opens, select the restore type: Device or Object.
5. (Only applicable for Proxy and Firewall) On the Restore screen that opens, the restore type is selected as Device by default.
6. Enter the device name.
7. In the date range field that appears below the Device name field, click the date you want to restore the device or object to.
8. Leave the default value in the **Restore to Field**, which should match the device or object name you entered in Step 7.
9. Click **Proceed**.
   The screen refreshes and displays a Configuration in the latest archive field, which should show the backup you selected. The table below it 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.




10. At the bottom of the screen, enter a reason for restoring to the backup.
11. Click **Restore**.

## Compare Configurations of Custom Environments

To compare configurations custom environments of an object:

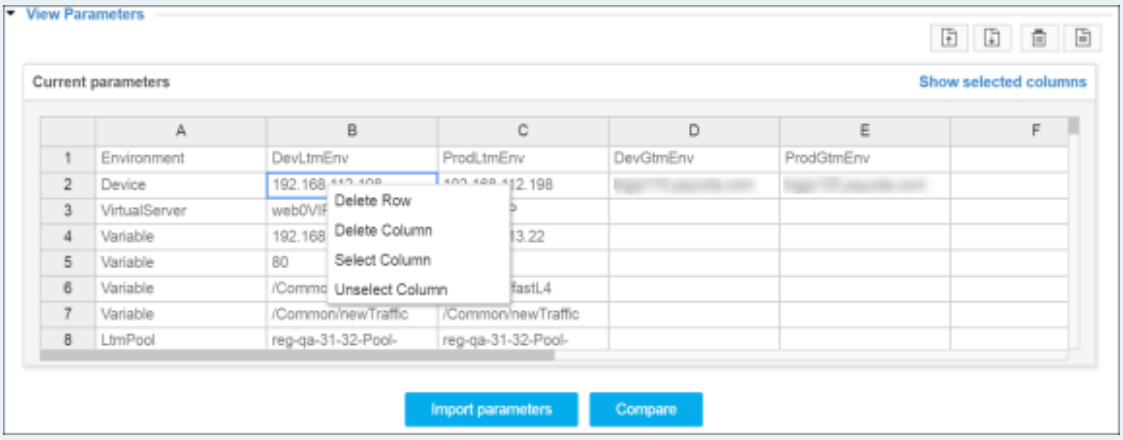
- You can only compare a maximum of two environments at a time.
- This feature is applicable only for F5 device objects.

**Note:** To add data to the table, you must download the sample file, fill in all the required environment details and the corresponding objects, and then import it.

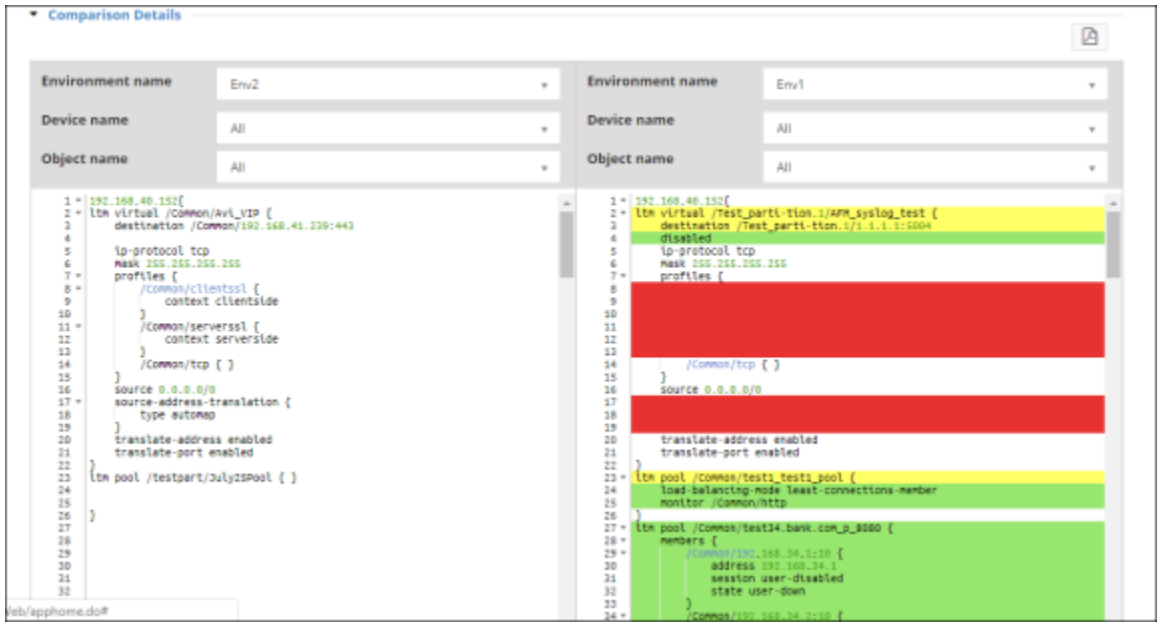
1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. Click the **Compare** tab.

3. In the Compare Type field, select the **Environment** radio button.
4. Click ▸ beside **View Parameters** section to expand it.
   The **Current Parameters** table is displayed.

**Note:** 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



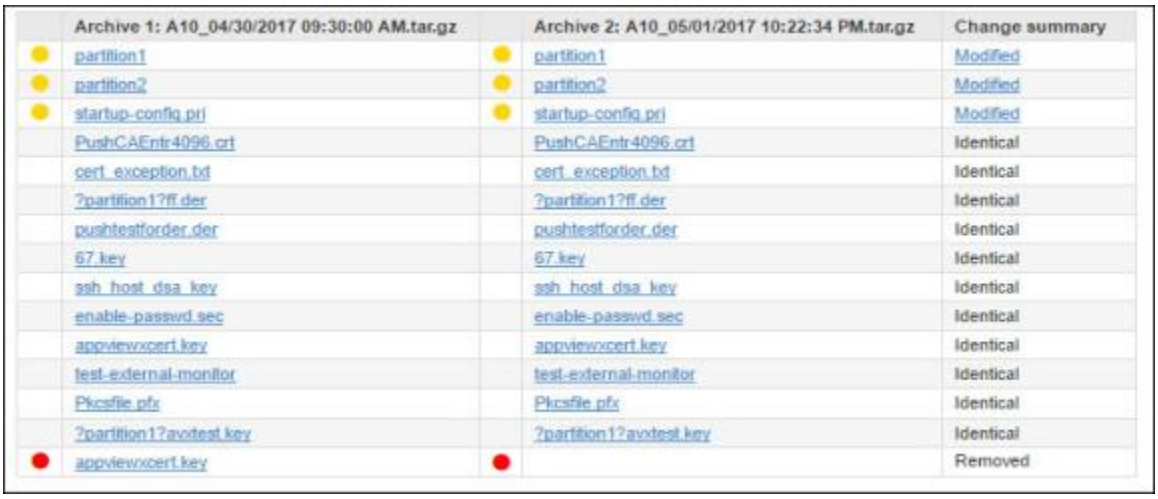

**Note:** If required, you can click to download the comparison report to your computer.

## Compare Device Backups

To compare backups for the same or different devices:

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. In the **Sub Systems** column on the left, click **ADC**,Proxy,or **Firewall**, depending on the device types that you want to compare.
3. Click the Compare tab.
4. (Only applicable for ADC) On the Compare screen that opens, select the compare type: Device or Object.
5. (Only applicablefor Proxy andFirewall) On the Compare screen that opens, the compare type is selected as Device by default.
6. In the Device name field, enter the name of the first device whose backup you want to compare.
7. In the Archive 1 field, select the first backup in the comparison.
8. 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.
9. In the Archive 2 field, select the second backup in the comparison.
10. Click Compare.

A table appears at the bottom of the screen, showing all of the files contained in the two backups you selected. Yellow circles appear beside each file that has been modified since the earlier backup was taken and red circles appear beside each file that has been removed since the earlier backup was taken.



| Archive 1: A10_04/30/2017 09:30:00 AM.tar.gz | Archive 2: A10_05/01/2017 10:22:34 PM.tar.gz | Change summary |
|---|---|---|
| partition1 | partition1 | Modified |
| partition2 | partition2 | Modified |
| startup-config.prj | startup-config.prj | Modified |
| PushCAEntr4096.crt | PushCAEntr4096.crt | Identical |
| cert_exception.txt | cert_exception.txt | Identical |
| ?partition1?ff.der | ?partition1?ff.der | Identical |
| pushtestforder.der | pushtestforder.der | Identical |
| 67.key | 67.key | Identical |
| ssh_host_dsa_key | ssh_host_dsa_key | Identical |
| enable-passwd.sec | enable-passwd.sec | Identical |
| appviewxcert.key | appviewxcert.key | Identical |
| test-external-monitor | test-external-monitor | Identical |
| Pkcsfile.pfx | Pkcsfile.pfx | Identical |
| ?partition1?avxtest.key | ?partition1?avxtest.key | Identical |
| appviewxcert.key | | Removed |

## Compare Multiple Configurations of an Object

To compare multiple configurations of an object,

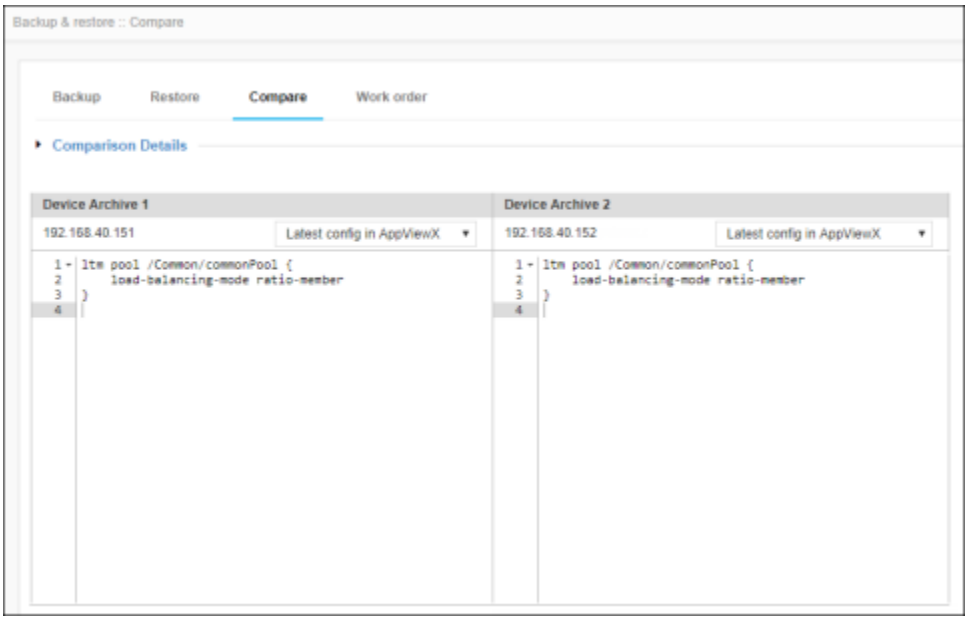
**Note:** You can only compare a maximum of five configurations at a time. This feature is applicable only for F5 device objects.

1. Click and select **Inventory** > **Backup & Restore**.
   The Backup & Restore screen opens.
2. Click the **Compare** tab.
3. In the Compare Type field, select the Object radio button.
4. Select the vendor whose objects you want to compare.
5. Select the object type you want to compare.
6. Click the Object Name dropdown list and select the name of the object whose configurations you want to compare.
7. 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.

**Note:** If you want to compare configurations of the same device over time, choose the device you selected in Step 7.

8. In the Archive Name field, select the first configuration you want to use in the comparison.
9. In the second Device name dropdown list, select the second device you want to use in the comparison.
10. In the second Archive Name field, select the configuration you want to compare the first configuration to.
11. Click + to add more configurations of an object.
12. Click **Compare**.

    The screen refreshes and displays the two archived configurations side-by-side.




## Edit the Settings of the Backup Screen

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

1. Click ☰ and select **Inventory** > **Backup & Restore**.

   The Backup & Restore screen opens.
2. If the Backup tab is not displayed by default, click to open it.
3. In the **Sub Systems** column on the left, click **ADC**, Proxy, or **Firewall**, depending on the device whose settings you want to modify.
4. Click ⚙ in the Command bar.
5. 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 16.
6. Select the Display warning messages when overwriting archives check box if you want users to be warned whenever they are about to overwrite an archive.
7. Click Submit to save the settings.

## Search for an Inventory Item

The search feature within the Inventory module allows you to run a basic search of all columns of data for any inventory item. Wildcards and Boolean operators, such as AND and OR, are not supported.

To search for an item:

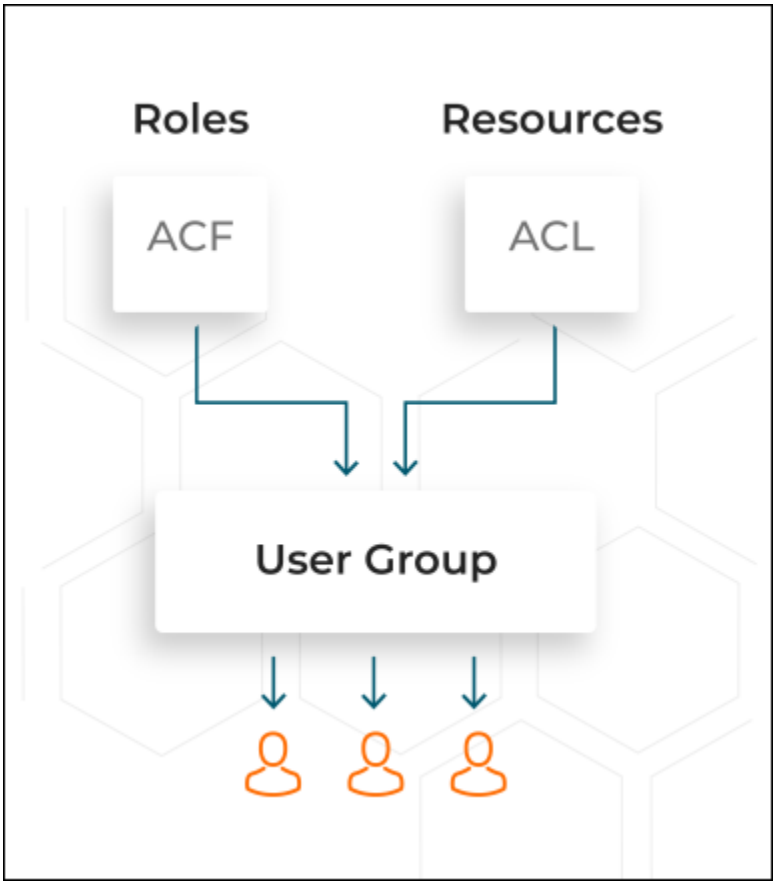
1. Click  .
2. Go to **Inventory** and then to the inventory component containing the type of item you want to search for: for example, to find an ADC, select the Device inventory component.
3. At the top of the screen, click the tab that corresponds to the type of device you want to search for: ADC, server, DNS, firewall, WAF, switch, router, proxy, or other.
4. In the Search field, enter a word, phrase, IP address, or any other text that is associated with the inventory item.
5. Click **Enter** on your keyboard to run the search.
6. In the results list, click the item name to view its complete details.

# Chapter 8: Account Module



## Introduction

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



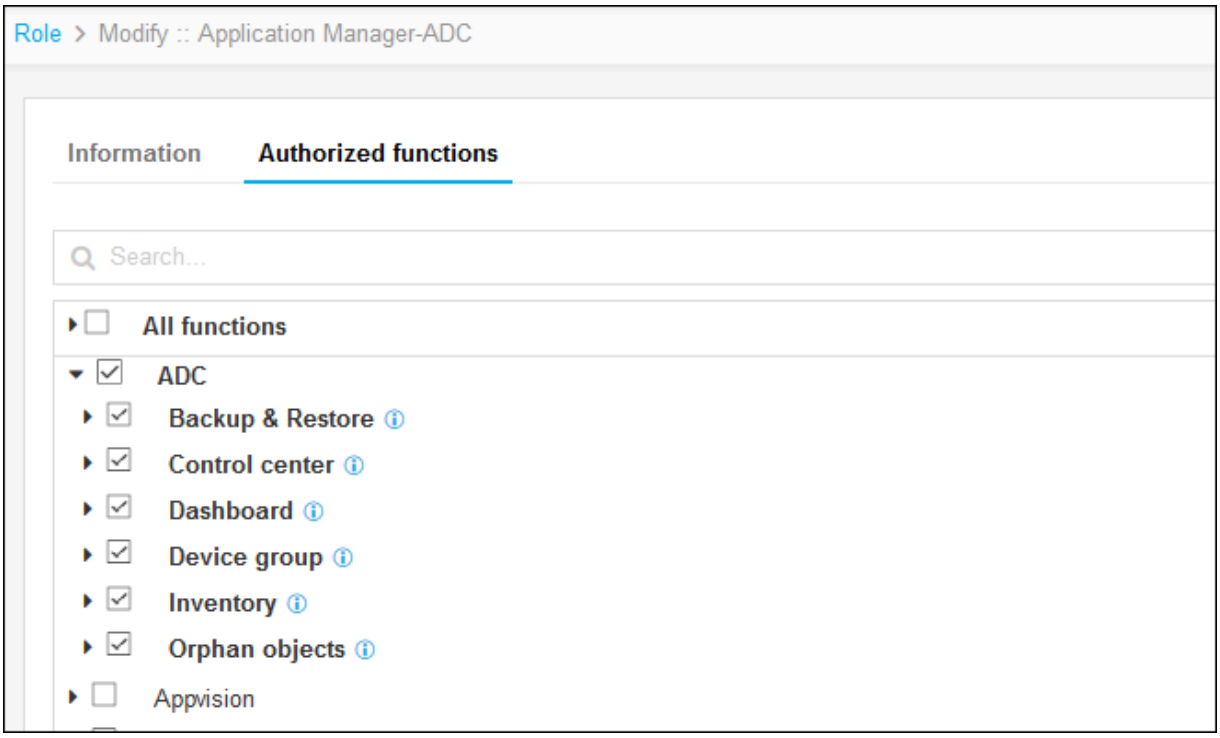
## Overview

A set of permissions to execute specific tasks in the application is termed as **Roles** in AppViewX. Roles can be assigned only to a user group. Users within user groups will inherit role permissions assigned to that group. User groups can be assigned more than one role. A default set of roles is available within the application as per the industry standards.

## Create a Role

To create a role:

1. Click  and select > **Account** > **Role**.
2. Click  on the top.
3. On the **Add** screen, under the **Information** tab, specify a role name such as Admin.
4. Enter a brief description of the role or features/functionalities that are associated with the role.
5. Click **Save**.
6. Click the **Authorized Functions** tab.
7. Select the checkbox beside the functionalities that you want to associate with the role.
8. To assign functions at a granular level, click the **expand** icon beside a function checkbox and then select individual sub-options within that function.
   For example, in the image below, you can select ADC that automatically assigns all six sub-options and options within sub-options or you can expand the ADC function and select only the sub-options you want to assign.




9. Click **Save**.

## Modify a Role

To modify a role in AppViewX:

1. Click and select > **Account** > **Role**.
2. On the roles list view, select the checkbox beside the role you want to modify and click .
3. On the **Modify** page, make required changes to fields on the **Information** and **Authorized Functions** tabs.
4. Click **Save**.

   Fields that are grayed out cannot be edited.

> **Note:** For more info on the functionality of these tabs, refer to Create a Role.

## Delete a Role

> **Note:** You cannot delete a role that has active users in it.

To delete a role from AppViewX:

1. Click and select > **Account** > **Role**.
2. On the roles list view, select the checkbox beside the role you want to delete.
3. Click .
4. On the confirmation screen that pops up, click **Yes**.

## Clone a Role

The Clone a role option allows you to create a 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.

To clone a role:

1. Click and select > **Account** > **Role**.
2. On the roles list view, select the checkbox beside the role you want to clone.
3. Click .
4. On the **Information** tab, enter a role name.
5. Enter a brief description of the role or features/functionalities associated with the role.
6. Click **Save**.

## Enable a Role

To enable a role in AppViewX:

1. Click and select > **Account** > **Role**.
2. On the roles list view, select the checkbox beside the role you want to enable.
3. Click .
4. On the confirmation screen that pops up, click **Yes**.

## Disable a Role

**Note:** You cannot disable a role that has active users in it. Users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

To disable a role in AppViewX:

1. Click and select > **Account** > **Role**.
2. On the roles list view, select the checkbox beside the role you want to disable.
3. Click .
4. On the confirmation screen that pops up, click **Yes**.

# Resource



## Overview

All the devices and objects that are configured within AppViewX are termed as Resources. Resources can be assigned to a user group. Users within a user group will inherit resources assigned to that group. User groups can be assigned more than a resource.

The following resource-related tasks can be performed within AppViewX:

- Create a resource
- Modify Read/Write permissions for components assigned to a Resource
- Delete a resource
- Clone a resource
- Enable a resource
- Disable a resource

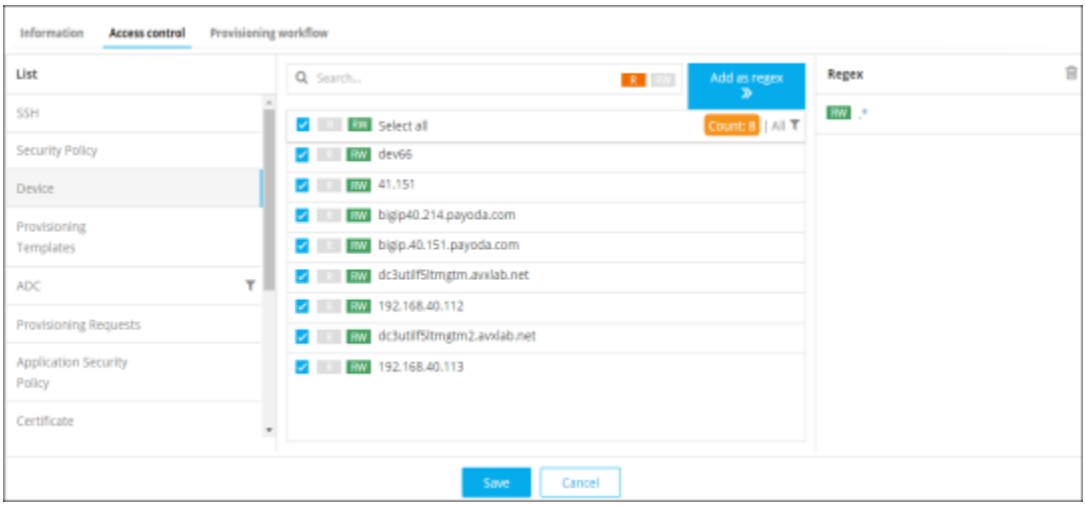
## Create a Resource

To create a resource:

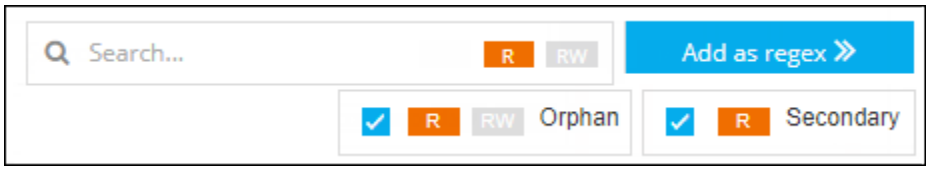
1. Click and select **Account** > **Resource**.
2. Click on the top.

3. On the **Add** details page, under the **Information** tab, enter a resource name.
4. Enter a brief description of the resource or the granular level access associated with the resource.
5. Click **Save**.
6. Click the **Access Control** tab on the top and select one of the following:
   - Device — You can click ⧩ to select devices to be displayed.
   - Certificate
   - ADC — You can click ⧩ to select device objects to be displayed.
   - SSH
   - Command Session Control
   - Provisioning Templates
   - Provisioning Requests
   - Security Policy
   - Application Security Policy
   - Proxy List
   - Blueprint
   - Application
   - Workflow Studio
   - Workflow Requests
7. To use a regular expression (regex) to identify devices you want to associate with the resource that you are creating:
   - Enter the regex in the **Search** field.
   - Click either the **R** (Read-only) or **RW** (Read/Write) to designate whether user groups assigned to the resource have read-only or read/write permissions on devices returned as search results.
   - Click **Add as Regex**. Devices list updates and show checkmarks beside all devices that match the regex to indicate that they have been selected. The Regex column also displays the total number of devices that match each of the regex search criteria you have created.
8. If you do not want to use a regex for each device in the list, click **R** (Read-only) or **RW** (Read/Write) to designate whether user groups assigned to the resource have read-only or read/write permissions on the device.

**Note:** The benefit of using a regex rather than selecting devices manually is that the search string continues to work in the background, auto-assigning all new devices to the resource if the devices match the regex you create.




9. After assigning a device to the role, click **Save**.
10. Repeat steps 6 through 9 for each of the remaining list on the **Access Control** page.
11. The ADC has two additional fields that allow you to assign global permissions for orphan and secondary ADC objects to the resource you are creating. Users cannot assign individual permissions to orphan and secondary objects. To enable this ability, complete the following sub-steps:
    a. Click the **ADC** tab.
    b. Under the Search field, select the checkbox beside Orphan to assign global permissions to orphan objects.




    c. Click either the R or RW icon to give users assigned to the resource Read-Only or Read/Write permissions on all orphan objects.
    d. Select the checkbox beside Secondary if you want to assign global permissions for secondary objects.
    e. Click the R icon to give user groups assigned to the resource Read-Only permissions on all secondary objects. The RW icon is not available because you cannot grant Read/Write access to secondary objects.
    f. Continue with the rest of the steps in the process, then click **Save**.
12. After assigning the role, click the **Provisioning Workflow** tab on the top. The provisioning workflow allows you to determine workflows you want to associate with the resource you are creating.

13. Select the checkbox beside each workflow you want to associate with the resource and click ▸ beside a workflow name to view and select approval levels you want to provide to the workflow.
14. Click **Save**.

## Modify Read/Write Permissions for Components Assigned to a Resource

To modify Read (R) and Read/Write (R/W) permissions of devices, device objects, certificate groups, provisioning requests or provisioning templates associated with a resource:

1. Click and select **Account** > **Resource**.
2. On the resources list view, select the checkbox beside the resource whose component Read/Write permissions you want to modify.
3. Click on the top.
   By default, the **Information** tab is selected.
4. Click the **Access Control** tab.
5. On the left-hand column, click to select any of the following—Device, Certificate, ADC, SSH, Workflow, Application, and so on that contain the object whose permissions you want to change.
6. Locate the object on the list in the middle of the screen, then click R or RW as required.
7. Click **Save**.

## Delete a Resource

To delete a resource from AppViewX,

1. Click and select **Account** > **Resource**.
2. On the resource list view, select the checkbox beside the resource you want to delete.
3. Click .
4. On the confirmation pop up window, click **Yes**.

## Clone a Resource

The Clone a resource option allows you to create an exact copy of an existing resource with a different name. The user can modify the access control permissions and the workflow components while cloning a resource.

To create a clone:

1. Click and select **Account** > **Resource**.
2. On the resources list view, select the checkbox beside the resource you want to clone.
3. Click on the top.
4. On the **Information** tab, enter a resource name.
5. Enter a brief description of the resource or the granular level access associated with the resource.
6. Click **Save**.

## Enable a Resource

To enable a resource in AppViewX:

1. Click and select **Account** > **Resource**.
2. On the resources list view, select the checkbox beside the resource you want to enable.
3. Click .
4. On the confirmation pop up window, click **Yes**.

## Disable a Resource

To disable a resource in AppViewX:

1. Click and select **Account** > **Resource**.
2. On the resources list view, select the checkbox beside the resource you want to disable.
3. Click .
4. On the confirmation pop up window, click **Yes**.

# User

- Overview
- Create a User
- Modify a User
- Delete a User
- Enable a User

## Overview

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).

To create user accounts, you must be assigned the **Administrator** role.

**Note:** You must add a user to the user group as the roles and resources cannot be directly associated with the user.

## Create a User

To create a user:

1. Click and select **Account** > **User**.
2. Click on the top.
   By default, the **Information** tab displayed.
3. Enter a **Username** for the new user.
4. Enter and then confirm a **Password** for the user. The following restrictions apply when creating a user password:
   • Have at least one uppercase and one lowercase character
   • Have at least one numeric character
   • Have at least one special character ~!@#$^&*_-+=|().
   • Be 6 to 24 characters long
   • Not contain the user name
   • Not contain the same character more than three times in a row (**Example:** aaaaL1$)
   • Not contain blank spaces
5. (Optional) Select the **Authenticate Externally** checkbox if you want authentication handled by an external enterprise server such as LDAP, RADIUS or TACACS that is configured with AppViewX.
6. (Optional) Enter the user's first and last name.
7. (Optional) Enter descriptive information about the user such as their work location, workgroup, specialty, or any other details.
8. (Optional) Select a preferred mode of contact: Email address or telephone.
9. Enter an email address for the user.

10. Enter a phone number for the user. This is required if you select the **Telephone** as the preferred mode of contact.
11. Click **Save**.
12. Click the **User Group** tab to add the user to a group.
13. Select the checkboxes beside each of the user groups you want to add the user to.

> **Note:** A user can be assigned to more than one group in the system. A user assigned to more than one group inherits all of the permissions of all of the groups to which he or she is added.

## Modify a User

To modify a user in AppViewX:

1. Click and select **Account** > **User**.
2. On the users' list view, select the checkbox beside the name of the user you want to modify.
3. Click .
4. On the **Modify** page, make the necessary changes to the user's basic information.
5. Click the **User Group** tab and then select additional groups or deselect existing groups for the user.
6. Click **Save**.

## Delete a User

To delete a user from AppViewX:

1. Click and select **Account** > **User**.
2. On the users' list view, select the checkbox beside the user you want to delete.
3. Click .
4. On the confirmation screen that pops up, click **Yes**.

## Enable a User

To enable a user in AppViewX:

1. Click and select **Account** > **User**.
2. On the users' list view, select the checkbox beside the user you want to enable.

3. Click  .
4. On the confirmation screen that pops up, click **Yes**.

## Disable a User

To disable a user in AppViewX:

1. Click  and select **Account** > **User**.
2. On the user's list view, select the checkbox beside the user you want to disable.
3. Click  .
4. On the confirmation pop up window, click **Yes**.

## Import Users

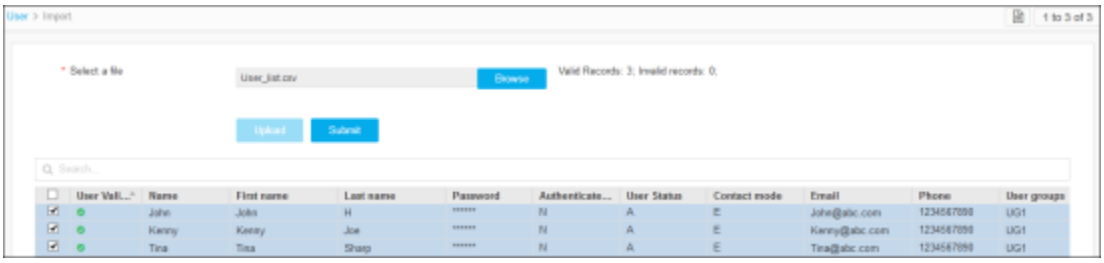
To import users into AppViewX:

1. Click  and select **Account** > **User**.
2. Click  on the top.
3. On the **Import** screen, click the **Browse** button and go to the location of the user file, select it and click **Open**.

**Note:** The file must be in .csv format. To download a sample template file click  on the top-right corner.

**Note:** The most efficient way to import user details is to download the sample import file that is available by clicking  in the Command bar of the Import screen, modify the contents, save it, and then import it into the system. This reduces the chance that error messages appear during the import process.

4. On the **Import** screen, click the **Upload** icon to see the user details displayed in the user interface. Note, at this point, the user details have not been imported yet: it's displayed for review.



5. Review the details of each user in the import file. If you do not want to import specific users, deselect the checkboxes beside their names.
6. Click **Submit**.

# User Group



## Overview

A user group is a set of individual users assigned with the same roles and resources. You can associate one or more roles and resource to a user group. Users within that user group are granted the role and resource permissions.

**Note:** You can associate roles and resources only with user groups.

## Create a User Group

To create a user group:

1. Click and select **Account** > **User Group**.
2. On the user group list view, click + on the top.
3. By default, the **Information** tab displayed.

4. Enter a name for the new user group.
5. (Optional) Enter a description of the group that makes it easy for administrators to determine whether a new user should be part of the group or not.
6. Click **Save**.
7. Click the **Roles** tab.
8. Select the checkboxes beside each role you want to assign to the new user group.
9. Click **Save** to associate a role with the user group.
10. Click the **Resources** tab.
11. Select the checkboxes beside each resource you want to assign to the new user group.
12. Click **Save** to associate a resource with the user group.

> **Note:** A user can be assigned to more than one role and resource in the system. A user assigned to more than one role or resource has all of the permissions of all of the roles and resources to which he or she is assigned. If one resource has only Read access to a component and another resource has Read/Write access to the same component, the higher-level access permissions (Read/Write) take precedence and the user has Read/Write access.

> **Note:** Admins who associate User Groups to Roles and Resources may skip/forget to associate User Groups to a user. To overcome this, an alert icon has been added to the User Group inventory to notify if the group is not associated with a role, resource, or both.

## Modify a User Group

To modify a user group in AppViewX:

1. Click  and select **Account** > **User Group**.
2. On the user groups list view, select the checkbox beside the group you want to modify.
3. Click  on the top.
4. On the **Modify** page, make necessary changes to the user group's basic information.
5. Click the **Roles** tab and then select additional roles or deselect existing roles for the user group.
6. Click the **Resources** tab and then select additional resources or deselect existing resources for the user group.
7. Click **Save**.

## Delete a User Group

To delete a user group from AppViewX:

1. Click and select **Account** > **User Group**.
2. On the user group list view, select the checkbox beside the group you want to delete.
3. Click on the top.
4. On the confirmation screen that pops up, click **Yes.**

> **Note:** You cannot delete a user group that has active users in it.

## Clone a User Group

Clone a User Group option allows you to create a copy of an existing user group with a different name. You can modify roles and resources associated while cloning a role.

To create a clone:

1. Click and select **Account** > **User Group**.
2. On the resources list view, select the checkbox beside the resource you want to clone.
3. Click on the top.
4. On the **Information** tab, enter a resource name.
5. Enter a brief description of the group that makes it easy for administrators to determine whether a new user should be part of the group or not
6. Click **Save**.

## Enable a User Group

To enable a user group in AppViewX:

1. Click and select **Account** > **User Group**.
2. On the group list view, select the checkbox beside the group you want to enable.
3. Click on the top.
4. On the confirmation screen that pops up, click **Yes**.

## Disable a User Group

You cannot disable a user group that has active users in it. Users who are associated with a disabled user group cannot log in to AppViewX.

To disable a user group in AppViewX:

1. Click  and select **Account** > **User Group**.
2. On the group list view, select the checkbox beside the group you want to disable.
3. Click  on the top
4. On the confirmation screen that pops up, click **Yes**.

# RBAC Quick Configuration

- Overview
- Authentication
- UserGroup
- Role
- Resource

## Overview

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

Quick Config wizard flow can also be accessed in the following ways:

- Navigate to **Menu** > **Account** > **User group** > **Quick Config** (or) click **Account** > **Role** > **Quick Config** (or) click **Account** > **Role** > **Quick Config**.
- The Authentication stage opens in a wizard flow with the LDAP sub-tab displayed by default. On the same screen as part of wizard flow, user groups, roles, and resources stages are displayed at the top. Click on the respective stage for configuration.

## Authentication

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

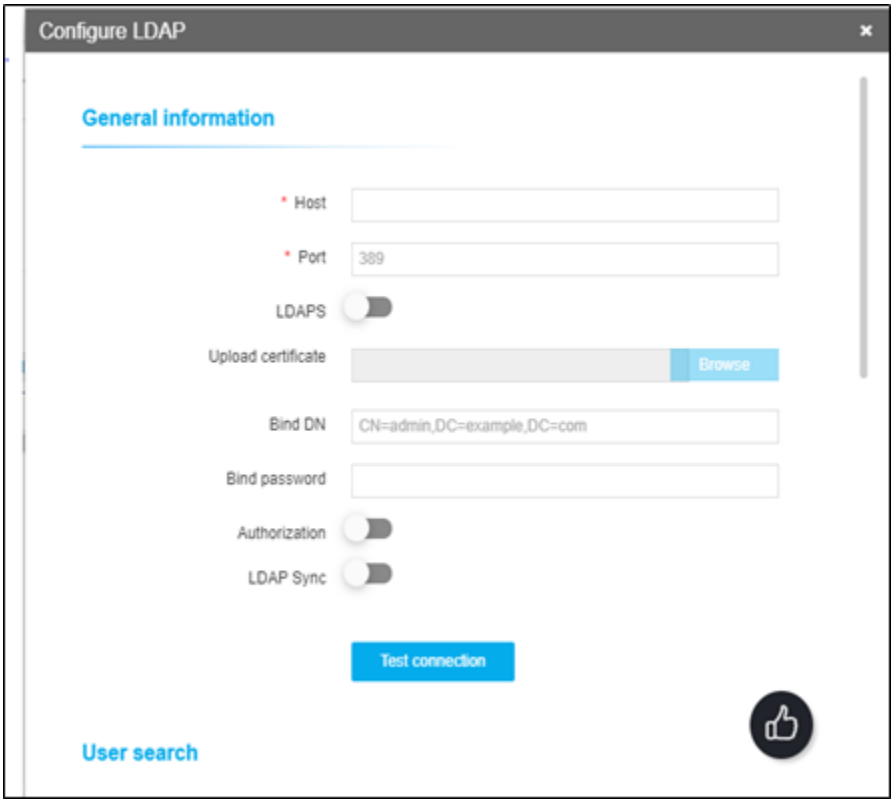
- LDAP
- TACACS

- RADIUS
- SAML
- Authentication Type Ordering and Enabling/Disabling

## LDAP

To configure the settings for LDAP or LDAPS authentication:

1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click **Configure LDAP**.
   Configure LDAP popup window appears.




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

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

    **Note:** You can test the connection of LDAPS only when you save all of the configuration details. Bind DN and Bind password details cannot be validated through a test connection.

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

16. The next three fields on the tab, Group search base, Group search filter, and Group return attribute, are related to those in steps 8–10 above. The difference is that the search and fetch group membership details and also provide authorization for the group that the user is associated with. For example, enter ou=secgrp,dc=sample,dc=com for the Group search base, 'member=*' for the Group search filter, and cn for the Group return attribute.

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

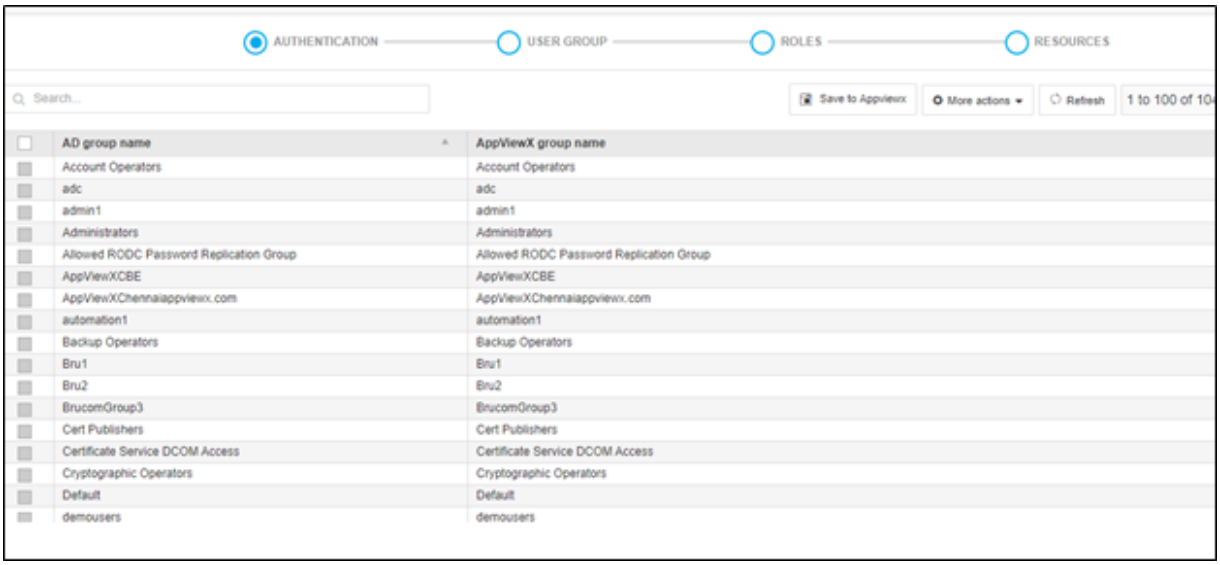
17. Click **Test Query** to check if it is a valid group.
18. In the Authorization map field, select how you want to map the return attribute:
    - Select the User group radio button to map the attribute to the user group.
    - Select the Role radio button to map the attribute to the role.
    - Click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

> **Note:** To delete an existing configuration in the LDAP inventory table, select the required LDAP configuration using the **Select** checkbox beside the respective configuration. Click on **More Actions** and from the drop-down options, click **Delete**.

> **Note:** To update an existing configuration in the LDAP inventory table, click on the **Host Hyperlink**, on the **Modify LDAP** popup window, update the required details. Then, click **Update**.

19. In the table, click **Fetch User Groups** that exist as the second column to view the user groups available in the AD and create or map them with the existing user groups in AppViewX.
20. In the popup screen that appears, fetch user groups specific to a user option selected by default, then type the username of an AD user.
21. To pull specific user groups by user group name from AD into AppViewX based on specific patterns/ keywords/code, select **Fetch User Groups** option, then type the user group name in AD.
22. Either an exact group name or using a wild character search(asterisk (*) - matches any number of characters. You can use * anywhere in a character string).
23. For example, to search User groups names containing ‘admin’, type user group name as ‘admin*’ in the search text box. All the user groups' names containing admin in AD will be retrieved.

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



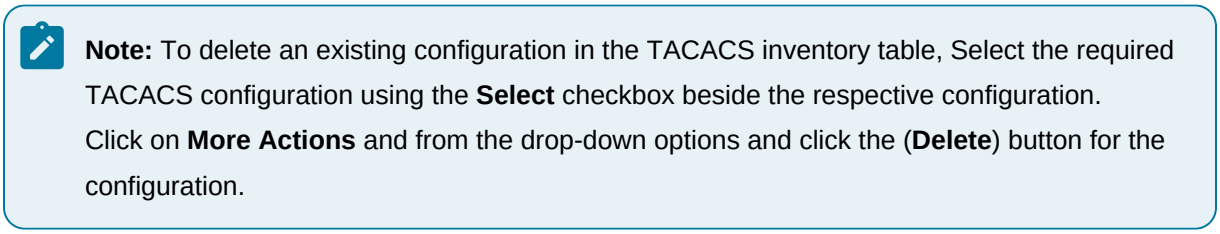

25. Select the AD user group(s) that must be created with the same name in AppViewX and click the **Save to AppViewX**.
26. You can also select the AD user group(s) to be mapped with the existing AppViewX user group and click the **More Actions>> Create Map** option in the dropdown. Select the required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

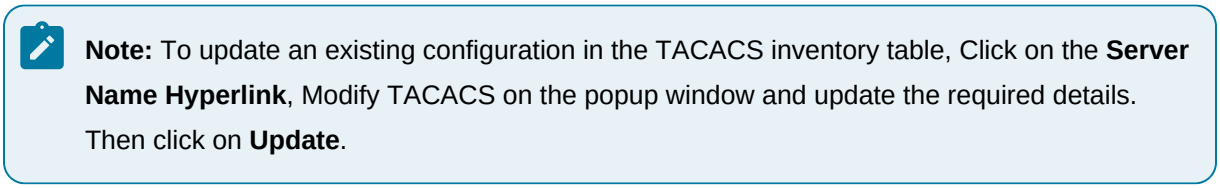
## TACACS

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

To configure the settings for TACACS authentication:

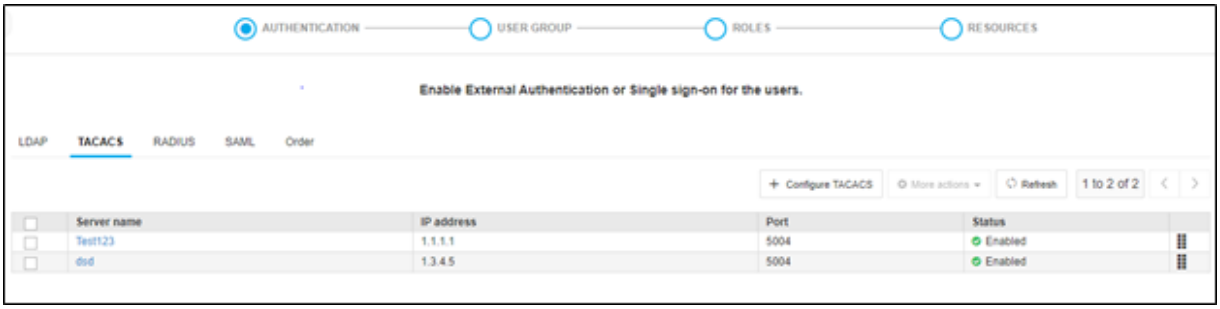
1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click the **TACACS** sub-tab and click on **Configure TACACS**.
3. Enter the name of the TACACS authentication server in the configuration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




11. To disable a server configured, select the required TACACS configuration and click on **More Options>> Disable** option from the dropdown to disable a configuration that is currently in the enabled status.
12. To enable a server configured, select the required TACACS configuration and click on **More Options>> Enable** option from the dropdown to enable a configuration that is currently in disabled status.
13. (Optional) Repeat steps 2 through 10 to add more TACACS servers to the system.
14. (Optional) In the servers inventory table, click and hold a server name and drag it up or down to change the order of TACACS servers in use in the system.

The order will be automatically saved.




## RADIUS

The AppViewX system allows you to add more than one Remote Authentication Dial-In User Service (RADIUS) server for authentication.

To configure the settings for RADIUS authentication:

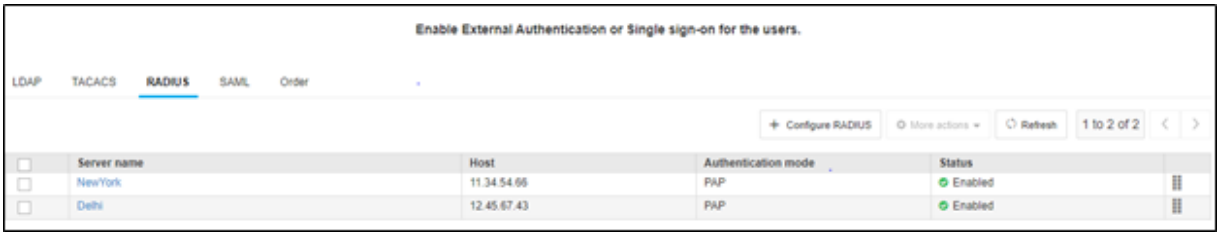
1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click the **RADIUS** sub-tab and click on **Configure RADIUS**.
3. In the Server name field, enter the name of the server you want to set up RADIUS authentication for in the configure pop up appears.
4. In the Host field, enter the IP address of the RADIUS server.
5. In the Shared secret field, enter the secret text string shared between the RADIUS server and AppViewX.
6. In the Authentication port field, enter a port number that AppViewX will use for authentication.
7. In the Acceptance port field, define a port number that AppViewX will use to accept the response from the RADIUS server.
8. In the Authentication Mode field, select the radio button beside the kind of authentication you want to use. This must be confirmed in the RADIUS server settings as well. AppViewX supports the following four authentication modes:
   - PAP/ASCII
   - CHAP
   - MS-CHAPv2
   - EAP-MD5
9. The Authorization toggle is enabled by default and hence, authorization is required. The authorization can be done using RADIUS or LDAP. If you want to disable authorization, click the (Enabled) button to set it to (Disabled).
10. The following options are displayed only when the feature is enabled:

- (For RADIUS) In the Vendor ID field, enter the vendor server ID, which can be found in the Vendor-Specific Attributes (VSA) within the RADIUS server settings or which you can get directly from the vendor. An example is 500.
- (For RADIUS) In the Vendor type field, enter the vendor type, which can be found in the Vendor-Specific Attributes (VSA) within the RADIUS server settings or which you can get directly from the vendor. An example is 102.
- (For LDAP) From the LDAP dropdown list, select an LDAP server, using which the authorization must be performed.
- Click Add to save the RADIUS configuration in the AppViewX system and have it added to the list at the RADIUS Inventory table.

**Note:** To delete an existing configuration in the RADIUS inventory table, select the required RADIUS configuration using the **Select** checkbox beside the respective configuration and click on **More Actions** and from the drop-down options click the **Delete** button for the configuration

**Note:** To update an existing configuration in the RADIUS inventory table, click on the **Server Name Hyperlink**, modify on RADIUS popup window and update the required details. Then click on **Update**.

11. To disable a server configured, select the required RADIUS configuration, click on **More Options>> Disable** option from the dropdown to disable a configuration which is currently in the enabled status.
12. To enable a server configured, select the required RADIUS configuration, click on **More Options>> Enable** option from the dropdown to enable a configuration that is currently in disabled status.
13. (Optional) Repeat steps 2 through 11 to add more RADIUS servers to the system.
14. (Optional) In the server inventory table, click and hold a server name and drag it up or down to change the order of RADIUS servers in use in the system.
    The order will be automatically saved.

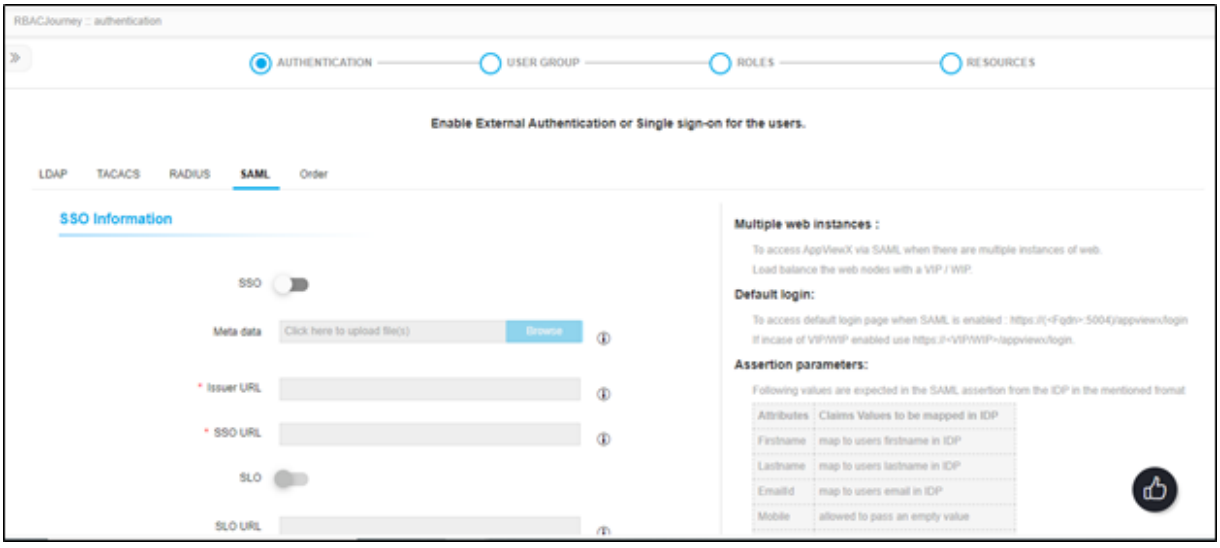


## SAML

The AppViewX system allows you to add more than one Security Assertion Markup Language (SAML) server for authentication.

To configure the settings for SAML authentication:

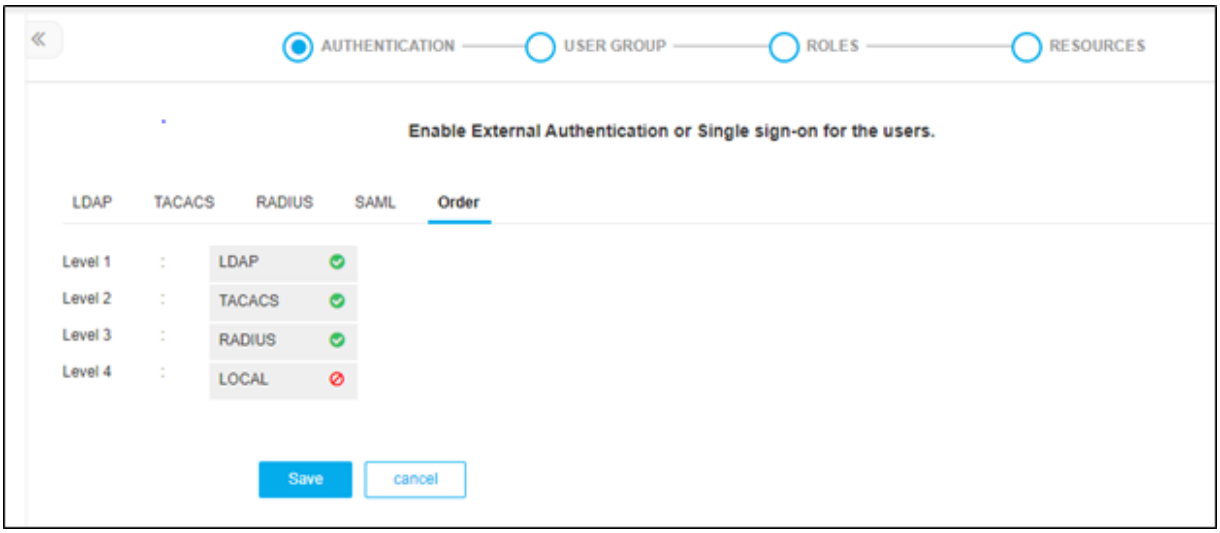
1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click the **SAML** sub-tab.
3. Click **Disabled** icon to enable the Single Sign-on (SSO).
4. (Optional) Click Browse to locate and select the metadata file containing the SSO configuration.
5. In the Issuer URL field, enter the entity ID of your Identity Provider (IdP).
6. In the SSO URL field, enter the protected endpoint provided by your IdP, to which, AppViewX sends the authentication request.
7. (Optional) Click the (Disabled) button to enable the Single Logout (SLO).
8. In the SLO URL field, enter your IdP protocol endpoint.
9. Click **Browse** to locate and select the required certificate.
10. Click **Save**.
11. Click **Copy** (in the Entity ID, Service URL, and SLO URL fields) and paste it in the respective field to configure the AppViewX details in your IdP server.




## Authentication Type Ordering and Enabling/Disabling

To set the order for the three different types of authentication within AppViewX and to enable or disable any of the types:

1. Click **Menu** > **Settings** > **General** > **Authentication** > **Quick Config**.
   The Authentication screen opens with the LDAP sub-tab displayed by default.
2. Click the **Order** sub-tab.
3. Re-order the authentication type levels by clicking a type and dragging it up or down in the list.




4. Enable or disable any of the authentication types by clicking the icon beside its name.
   - If the (Enabled) icon is showing and you click it, the authentication type is disabled.
   - If the (Disabled) icon is showing and you click it, the authentication type is enabled.
5. Click **Save.**

## UserGroup

A user group is a group of individuals that have access to the same roles and resources. When you associate a role and resource with a user group, the users within that user group are granted all of the roles and resource's corresponding privileges and permissions. User Groups can be created manually or synced from the active directory or can be bulk uploaded using a spreadsheet.

**Note:** You can associate the roles and resources only with the User groups.

Once Authentication details are configured, navigate to the **User Group** stage as part of the wizard flow to add user groups into AppViewX.

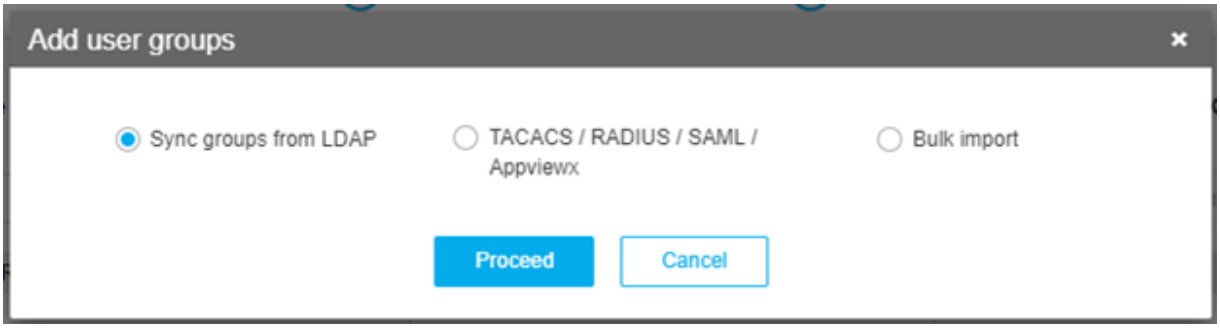
- Clicking on the **User Group** stage, the User group inventory table is displayed with the list of available user groups in AppViewX along with corresponding roles and resources mapping.
- In the User group stage, User group creation can be done by fetching groups from LDAP or can be bulk import, deletion of existing user groups, a clone of existing user groups, enable/disable of user groups can be performed.



## Add New User Group by Sync Groups from LDAP Option

To create a user group by sync groups from LDAP:

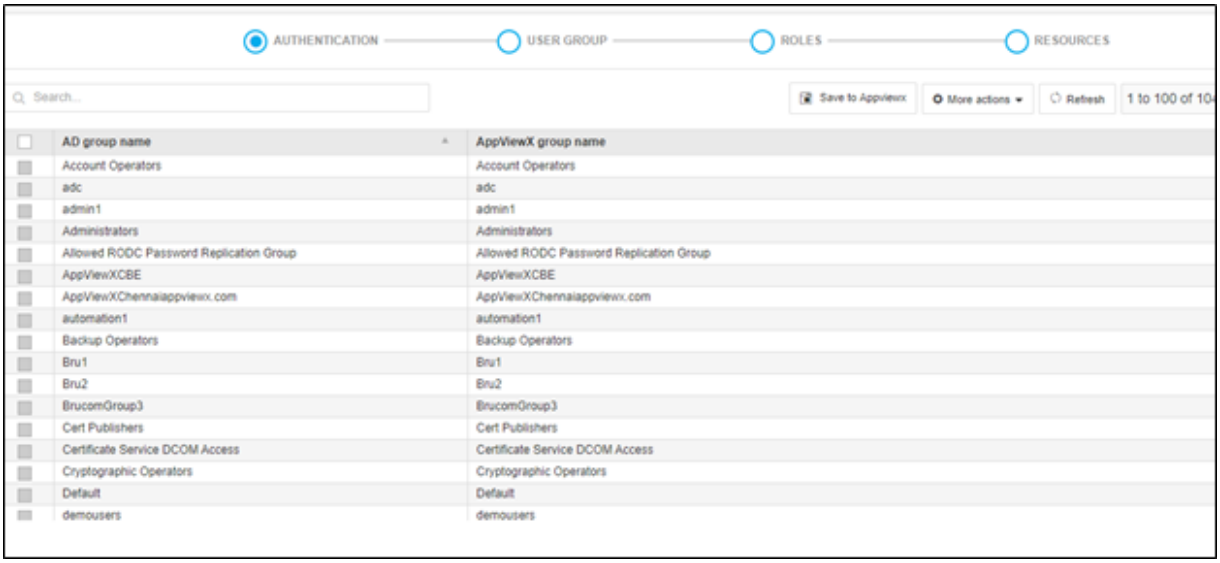
1. Click ☰ and select **User Group** > **Quick Config**.
   The Authentication stage part of RBAC Configuration wizard flow displayed by default.
2. Go to User group stage as part of the RBAC Configuration wizard flow.
3. Click the **Add New Group**.
4. Select **Sync Groups from LDAP** option and click on **Proceed**.




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

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

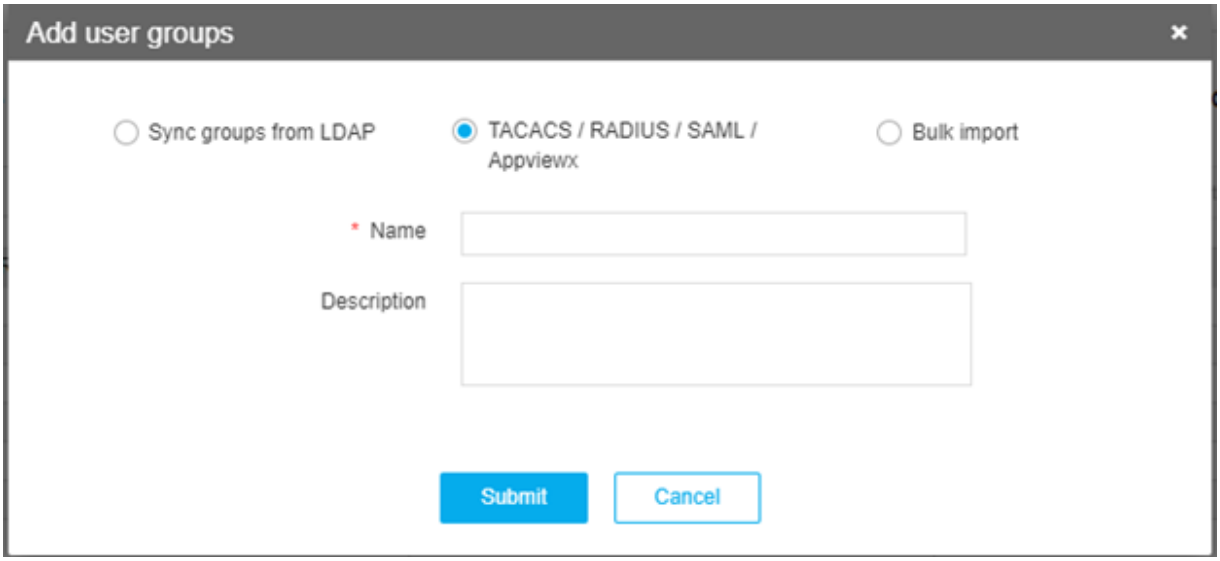
8. Click **Fetch**.
   A table containing the AD group names and their corresponding AppViewX user group names is displayed.




9. Select the AD user group(s) that must be created with the same name in AppViewX and click the Save to AppViewX button.
10. You can also select the AD user group(s) to be mapped with the existing AppViewX user group and click the **More Actions** > **Create Map** option in the dropdown.
11. Select the required existing AppViewX user group to be mapped from the **Mapping User Group** popup and click **Save**.
    Selected AD user group(s) will be now mapped to the existing AppViewX user group and the same mapping will be reflecting AD group names table.
12. You can also export the specific fetched AD groups by selecting specific **AD groups** by clicking **More Options** > **Export**.
13. From the export user groups popup, select **Selected group(s)** option and click **Yes**.
    The selected user group(s) should be automatically exported in (.CSV) format.
14. You can also export all the fetched AD groups by clicking **More Options** > **Export**.
15. From the export user groups popup, select the **All User Group(s)** option and click **Yes**.
    All user group(s) should be automatically exported in .CSV format.
16. To go back to the user group inventory table, click on **User Groups** breadcrumb at the top-left to view the onboarded user groups into AppViewX.

## Add New User Group by TACACS/RADIUS/SAML/AppViewX Option

1. Click ☰ and select **User Group** > **Quick Config**.
   The Authentication stage part of RBAC Configuration wizard flow displayed by default.
2. Go to User group stage as part of the RBAC Configuration wizard flow.
3. Click **Add New Group**.
4. Select **TACACS/RADIUS/SAML/AppViewX** option.
5. Enter a name for the new user group.
6. (Optional) Enter a description of the group that makes it easy for administrators to determine whether a new user should be part of the group or not.

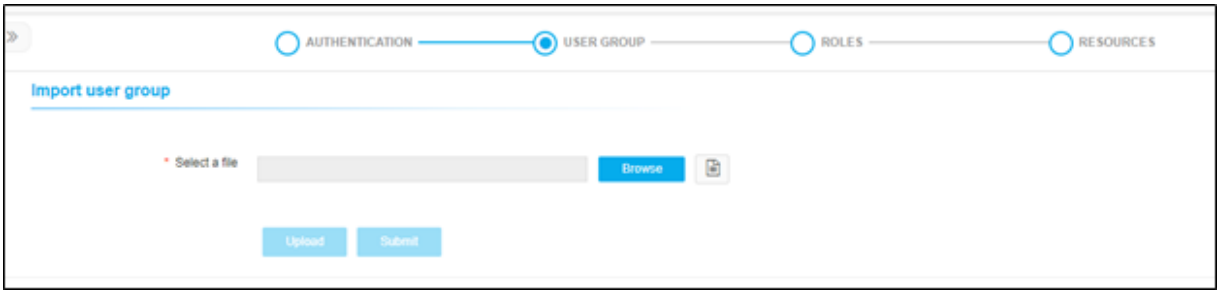



7. Click **Submit** to add user groups.

## Add New User Group by Bulk Import Option

1. Click ☰ and select **User Group** > **Quick Config**.
   The Authentication stage part of RBAC Configuration wizard flow displayed by default.
2. Go to User group stage as part of the RBAC Configuration wizard flow.
3. Click **Add New Group**.
4. Select the **Bulk Import** option.
5. Download a sample .CSV file if required to enter the list of user groups to be added in AppViewX.
6. Upload the.CSV file by clicking **Browse**.
7. Select the file from the respective location in your local PC from the popup that appears.
8. Click on Open in the popup once the file is selected.

9. Once the valid file is successfully selected, then Click on Upload in the Bulk Import page.




User group validation is performed on Imported user groups and displayed with validation status as Valid/Invalid.

> **Note:** Invalid status for a few user groups are displayed due to reasons like Duplicate Group name already exists, User group name provided doesn't meet the minimum criteria required to be added into AppViewX.

10. Select the list of user groups and click on **Save to AppViewX** to save the user groups from the imported file.
11. Even the user can select all user groups and click on "Save to AppViewX", only valid status user groups will be saved into AppViewX.
12. Once you go back to the User group inventory table, you need to re-upload the file to add user groups.

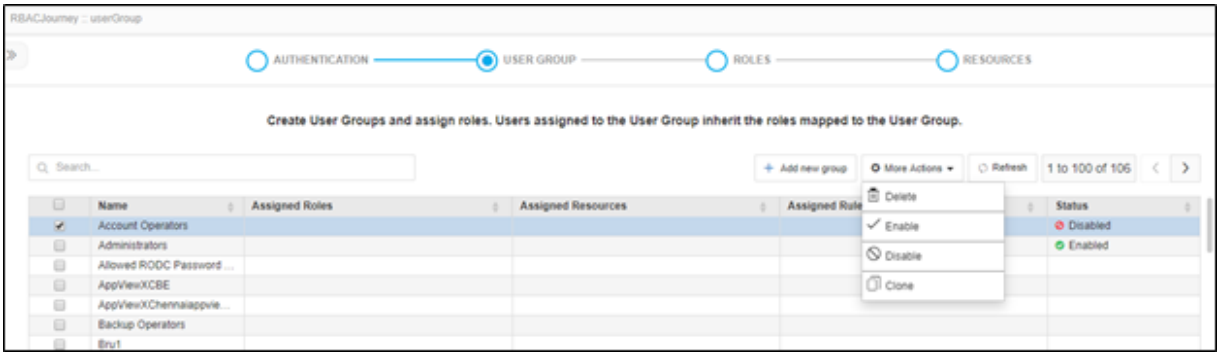
## Delete a User Group

To delete a user group from AppViewX:

> **Note:** You cannot delete a user group that has active users in it.

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to User group stage as part of the RBAC Configuration wizard flow.
3. In the user group list, select the checkbox beside the group you want to delete.
4. Click the **Delete** option in the **More Actions** dropdown.

5. On the confirmation screen that pops up, click **Yes**.




## Clone a User Group

The Clone a 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 associated while cloning a role.

To create a clone, complete the following steps:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to User group stage as part of the RBAC Configuration wizard flow.
3. In the user group list, select the checkbox beside the user group you want to clone.
4. Click the (Clone) option in the More Actions dropdown.
5. On the Clone popup, enter a user group name.
6. Enter a brief description of the group that makes it easy for administrators to determine whether a new user should be part of the group or not.
7. Click **Save**.

## Enable a User Group

To enable a usergroup in AppViewX:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to User group stage as part of the RBAC Configuration wizard flow.
3. In the group list, select the checkbox beside the group you want to enable.
4. Click the (Enable) option in the More Actions dropdown.
5. On the confirmation screen that pops up, click Yes.

## Disable a User Group

**Note:** You cannot disable a user group that has active users in it.

**Note:** Users who are associated with a disabled user group cannot log in to AppViewX.

To disable a usergroup in AppViewX:

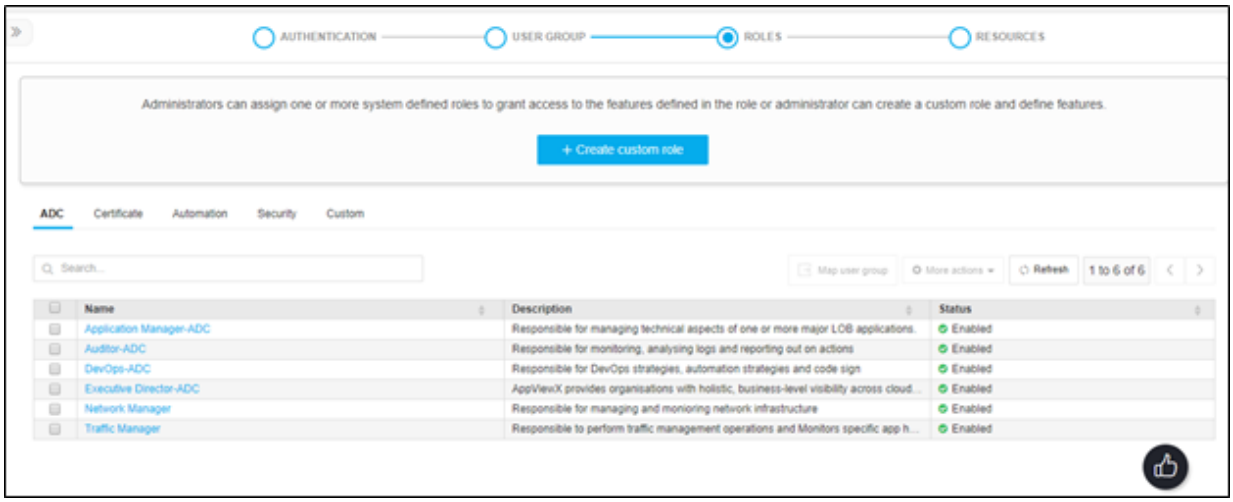
1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to User group stage as part of the RBAC Configuration wizard flow.
3. In the group list, select the checkbox beside the group you want to disable.
4. Click the **Disable** option in the More Actions dropdown
5. On the confirmation screen that pops up, click **Yes**.

## 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 more than one role.

Once User group details are added into AppViewX, go to the **Roles** stage as part of wizard flow into AppViewX to perform the following functions:

- Out of the Box (OOB) roles are available for ADC, Certificates, Security, and Automation modules.
- **OOB** roles can be cloned, enabled, and disabled. OOB roles can't be updated/deleted.



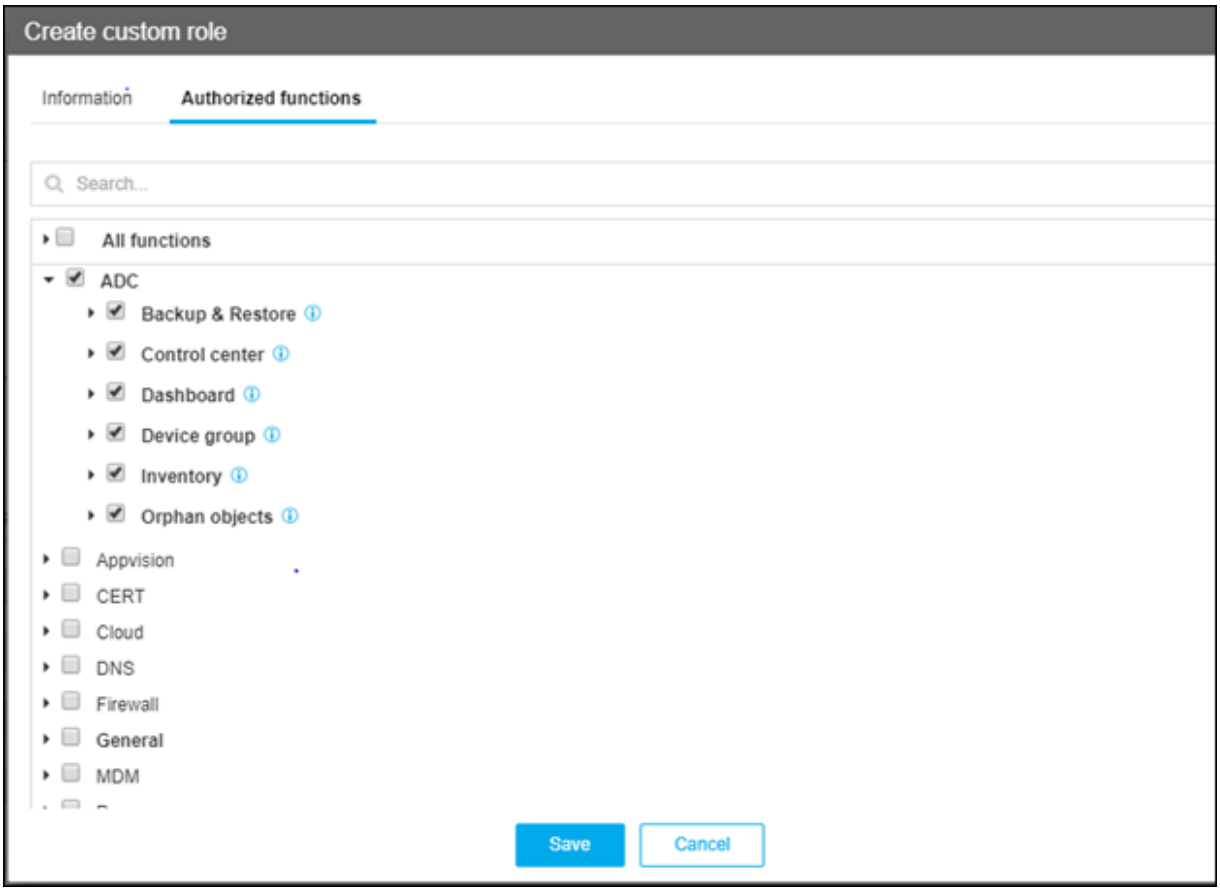
- Administrators can also create custom roles. Custom roles can be updated, deleted, enabled, and disabled.
- Users can either use **OOB** roles (if suits their needs) or custom roles to map to user groups.



## Create a Custom Role

To create a custom role:

1. Click  and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. Click **Create Custom Role**.
   The Create Custom Role screen opens.
4. On the **Information** tab, specify a role name, such as Admin.
5. Enter a brief description of what users assigned to the role can do and/or what features or functionalities are associated with the role.
6. Click **Save**.
7. Click the **Authorized Functions** tab.
8. Select the checkboxes beside each of the functionalities that you want to associate with the role that you are creating.
9. 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 suboptions 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.




10. Click on Information help icon against each ACF explaining the significance of the functionality.
11. Click **Save**.

## Modify a Role

To modify a role in AppViewX:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. On the roles list, click on the role name hyperlink you want to modify. The **Edit Role** screen appears.
4. Make whatever changes you want to the fields on the Information and Authorized functions tabs.

> **Note:** Fields that are grayed out, such as the Name field on the Information tab, cannot be edited.

5. Click **Save**.

> **Note:** Out of the box role functions can't be edited. Only custom role functions can be edited.

## Delete a Role

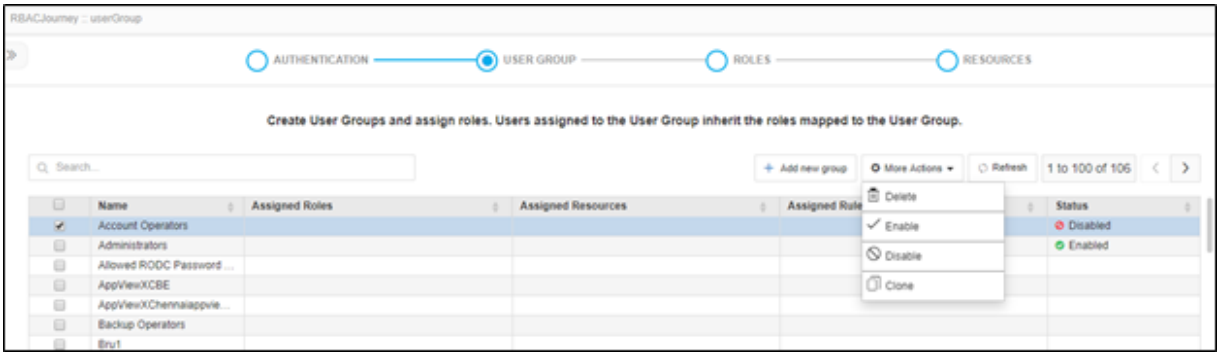
> **Note:** You cannot delete a role that has active users in it.

To delete a role from AppViewX:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. On the roles list, select the checkbox beside the role you want to delete under the custom roles tab.
4. Click **Delete** under **More Options** dropdown.

> **Note:** Out of the box roles can't be deleted. Only custom roles can be deleted.

5. On the confirmation screen that pops up, click Yes.




## 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.

To create a clone:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.

3. On the roles list, select the checkbox beside the role you want to clone.
4. Click **Clone** under **More Options** dropdown.
5. On the **Information** tab, enter a role name.
6. Enter a brief description of what users assigned to the role can do and/or what features or functionalities are associated with the role.
   Authorized functions will be pre-selected based on the cloned role. Make additional changes if required.
7. Click **Save**.

## Enable a Role

To enable a role in AppViewX:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. On the roles list, select the checkbox beside the role you want to enable.
4. Click **Enable** under **More Options** dropdown.
5. On the confirmation screen that pops up, click **Yes**.

## Disable a Role

**Note:** You cannot disable a role that has active users in it.

**Note:** The users associated with a disabled role through a user group will not be allowed to log in to AppViewX.

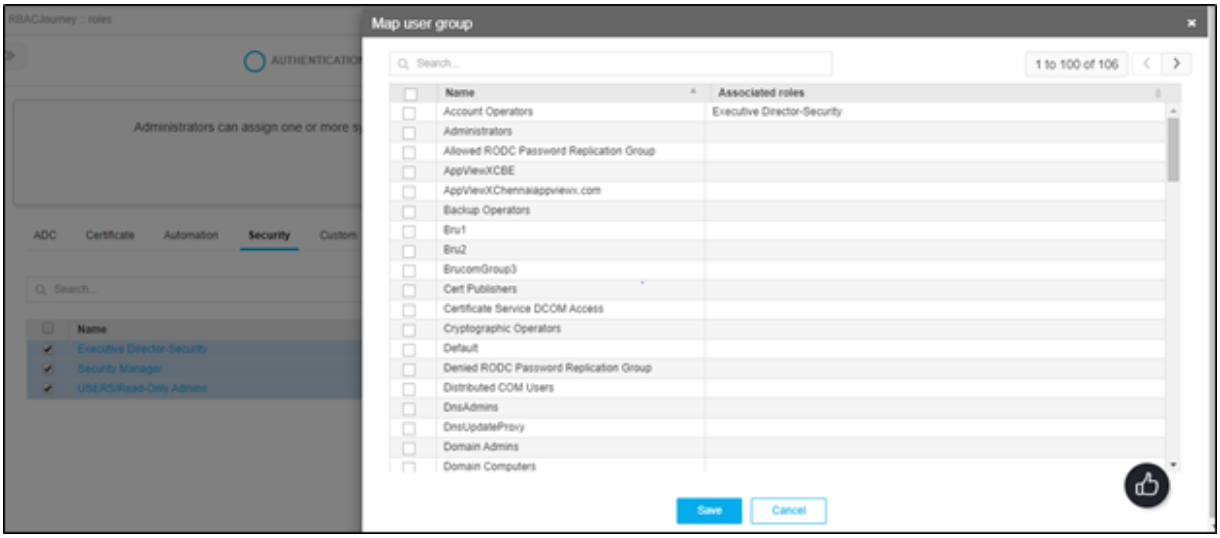
To disable a role in AppViewX:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. On the roles list, select the checkbox beside the role you want to disable.
4. Click **Disable** under **More Options** dropdown.
5. On the confirmation screen that pops up, click **Yes**.

## Role Mapping to User Groups

To map a role to user groups:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to Roles stage as part of the RBAC Configuration wizard flow.
3. On the roles list, select the checkbox beside the role(s) you want to map to user groups.
4. Click on the **Map User Group** option.
5. Select the required list of the user group(s) to be mapped for the selected role(s) in the **Map User Group** pop up.
6. Click **Save.**




## Resource

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 resources that are assigned to the user groups will automatically inherit the permissions associated with that resource. User groups can be assigned more than one resource.

Once roles are mapped to user groups, go to the **Resources** stage as part of wizard flow into AppViewX to perform the following functions:

- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query using object/Certificate fields available within in 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 option to dynamically tag ADC objects

**Note:** This dynamic resource tagging is only for newly discovered ADC objects, certificates.

**Note:** Objects/Certificates and respective permissions part of the existing resources will not be updated/changed.

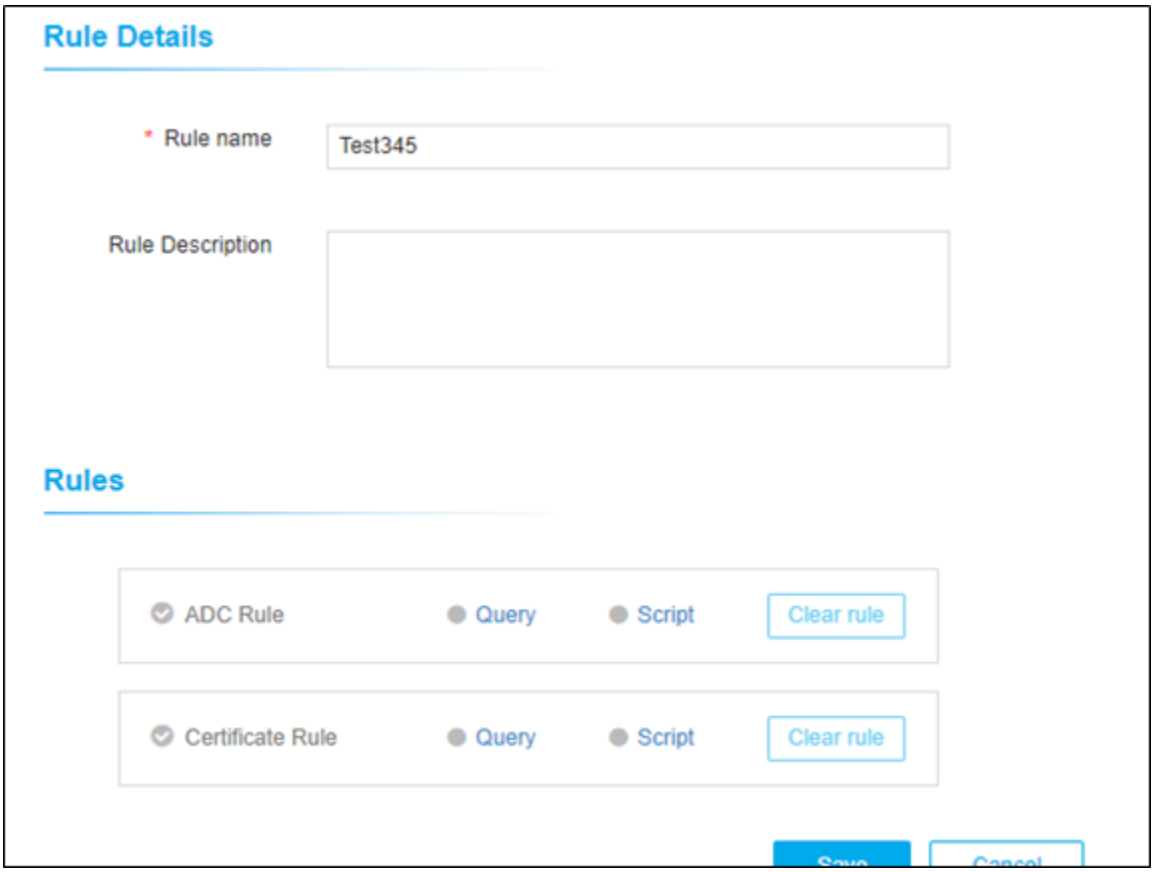


## Create an RBAC Rule to Tag ADC Objects Using a Query

To create an RBAC rule to tag resources using a Query:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. Click **Create Rule** from the **Rules** tab.


4. In the **Rule Name** box, enter a name for the rule.
5. (Optional) In the Description, enter additional information about the rule. Under Rules, an option to configure ADC Rule and Certificate rule using Query/Script will be available.




6. Click on **Query** hyperlink near the ADC rule to configure a rule to dynamically tag ADC objects using Query.
7. Configure the filter conditions for each ADC vendor by clicking on respective vendor-->Click on Add Filter.
8. Select the field, condition and enter the value to be monitored for dynamic tagging of ADC objects based on rule condition.

## Configuring a Variable as a Filter condition value part of the rule to dynamically tag objects based on patterns

A variable can be defined with a pattern as below:

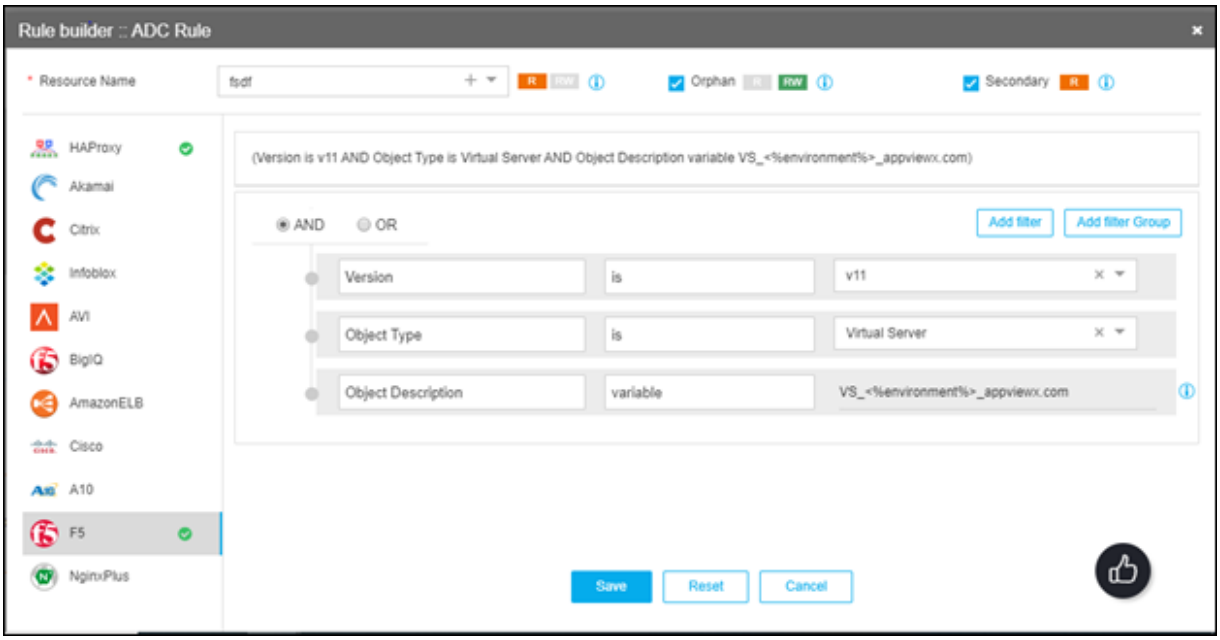
1. Select any one required field, then select condition as “Variable”, define value in the format of <%variable%>.
   Example: A virtual server configured with the pattern vs_prod_support.appviewx.com can be defined as vs_<%variable1%>_support.appviewx.com [where <%variable1%> can match to name UAT, DEV, etc.]
2. Multiple variable definitions for the same object pattern can be defined as. vs_<%variable1%>_<%variable2%>_support.appviewx.com [where <%variable1%> can match to name UAT,DEV etc and <%variable2%> can match to name sales,marketing etc ].
3. But variable can be used only across one field in a Rule.
4. Variable name should follow the below standards :
   - only alphanumerics [A-Z, a-z, 0-9]
   - special characters underscore [ _ ]
   - Placeholder is <% for beginning and %> for ending.
5. Specify a resource name.

## Configuring the Resource Name to Create Resources Dynamically based on Patterns

- Providing Resource Name of an existing resource by choosing the Resource Name from Drop Down.
- Providing a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
- Providing a Pattern for the Resource Name. [Provide the variable pattern defined in the Query as the Resource Name]. For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>.
- Then Click either the R (Read-only) or RW (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the ADC objects.
- The ADC objects tagging has two additional fields that allow you to assign global permissions for orphan and secondary ADC objects to the resource you are creating. Users cannot assign individual permissions to orphan and secondary objects.

To enable this ability:

1. Next to the **Resource name**, select the checkbox beside **Orphan** if you want to assign global permissions for orphan objects.
2. Click either the **R** or **RW** icon to give users assigned to the resource Read-Only or Read/Write permissions on all orphan objects.
3. Select the checkbox beside **Secondary** if you want to assign global permissions for secondary objects.
4. Click the **R** icon to give user groups assigned to the resource Read-Only permissions on all secondary objects. The **RW** icon is not available because you cannot grant Read/Write access to secondary objects.



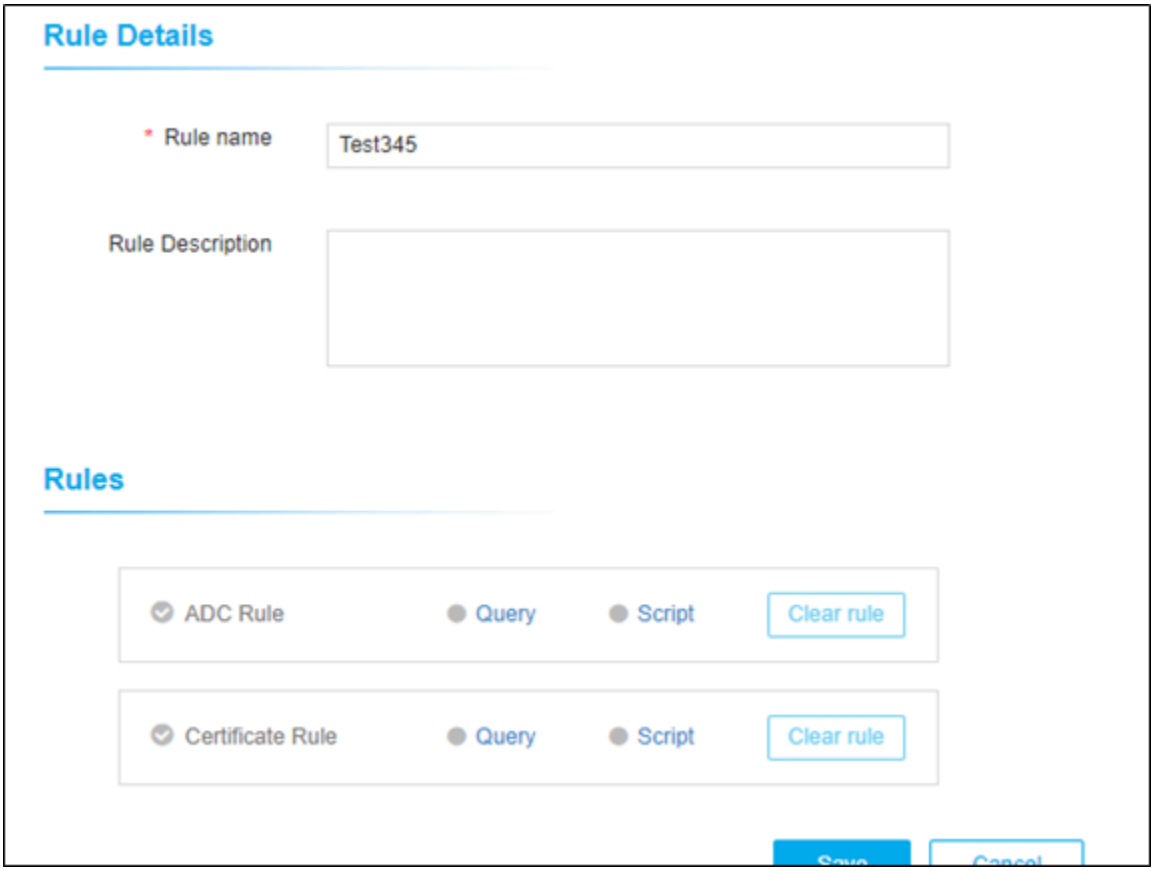

5. Click **Save**.
6. Saved rules will be displayed in the Rules tab. Go to the **Rules** tab by clicking on **Resource** in the breadcrumb.
7. Rule Summary details (Rule Name, Description, Rule Outcome) displayed in the Rule Inventory table.
8. Enable the rule by clicking on the respective status icon for the rule to be actively running.

## Create an RBAC Rule to tag Certificates using a Query

To create an RBAC rule to tag resources using a Query:

1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. Click **Create Rule** from the **Rules** tab.

4. In the **Rule Name** box, enter a name for the rule.
5. (Optional) In the Description box, enter additional information about the rule.
6. Under **Rules**, an option to configure ADC Rule and Certificate rule using Query/Script will be available.




7. Click on **Query** hyperlink near the Certificate rule to configure a rule to dynamically tag Certificates using Query.
8. Configure the filter conditions to dynamically tag certificates by clicking on **Add Filter.**
9. Select the field, condition and enter the value to be monitored for dynamic tagging of certificates based on rule condition.

- Configuring a Variable as a Filter condition value part of the rule to dynamically tag certificates based on patterns
- Configuring the Resource Name to Create Resources Dynamically based on Patterns

## Configuring a Variable as a Filter condition value part of the rule to dynamically tag certificates based on patterns

A variable can be defined with a pattern as below:

1. Select any one required field, then select condition as “Variable”, define value in the format of <%variable%>.
   Example: Certificate configured with the pattern Cert_SME_.appviewx.com can be defined as Cert_<%variable1%>_.appviewx.com [where <%variable1%> can match to name Subject Organization, Common Name, etc.]
2. Multiple variable definitions for the same object pattern can be defined as. Cert_<%variable1%>_<%variable2%>_.appviewx.com [where <%variable1%> can match to name Subject Organization, Common Name etc and <%variable2%> can match to name sales,marketing etc ].
3. But variable can be used only across one field in a Rule.
4. Specify a Certificate Group Name.
5. Variable name should follow the below standards:
   - only alphanumerics [A-Z, a-z, 0-9]
   - special characters underscore [ _ ]
   - Placeholder is <% for beginning and %> for ending.
6. Configuring the Certificate Group Name can be done in below ways to create Certificate Groups dynamically based on patterns:
   - Providing Certificate Group Name of an existing resource by choosing the Certificate Group Name from Drop Down.
   - Providing a Static Name to the Certificate Group Name. [When Rule matches the Resource Name would be created on Demand]
   - Providing a Pattern for the Certificate Group Name. [Provide the variable pattern defined in the Query as the Certificate Group Name]

     For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>

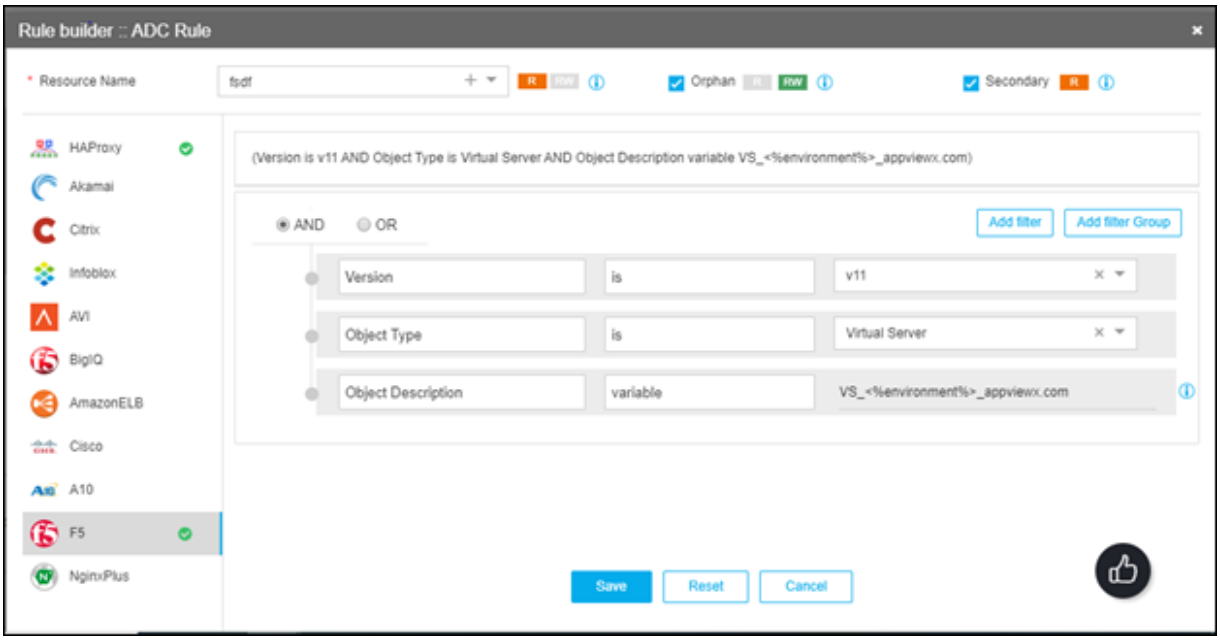
## Configuring the Resource Name to Create Resources Dynamically based on Patterns

- Providing Resource Name of an existing resource by choosing the Resource Name from Drop Down.
- Providing a Static Name to the Resource. [When Rule matches the Resource Name would be created on Demand].
- Providing a Pattern for the Resource Name. [Provide the variable pattern defined in the Query as the Resource Name]. For example, Resource_<%variablename%> | <%variablename%>_Resource | <%variablename%>.

- Then Click either the R (Read-only) or RW (Read/Write) button to designate whether user groups assigned to the resource have read-only or read/write permissions on the ADC objects.
- The ADC objects tagging has two additional fields that allow you to assign global permissions for orphan and secondary ADC objects to the resource you are creating. Users cannot assign individual permissions to orphan and secondary objects.

To enable this ability:

1. Next to the **Resource name**, select the checkbox beside **Orphan** if you want to assign global permissions for orphan objects.
2. Click either the **R** or **RW** icon to give users assigned to the resource Read-Only or Read/Write permissions on all orphan objects.
3. Select the checkbox beside **Secondary** if you want to assign global permissions for secondary objects.
4. Click the **R** icon to give user groups assigned to the resource Read-Only permissions on all secondary objects. The **RW** icon is not available because you cannot grant Read/Write access to secondary objects.

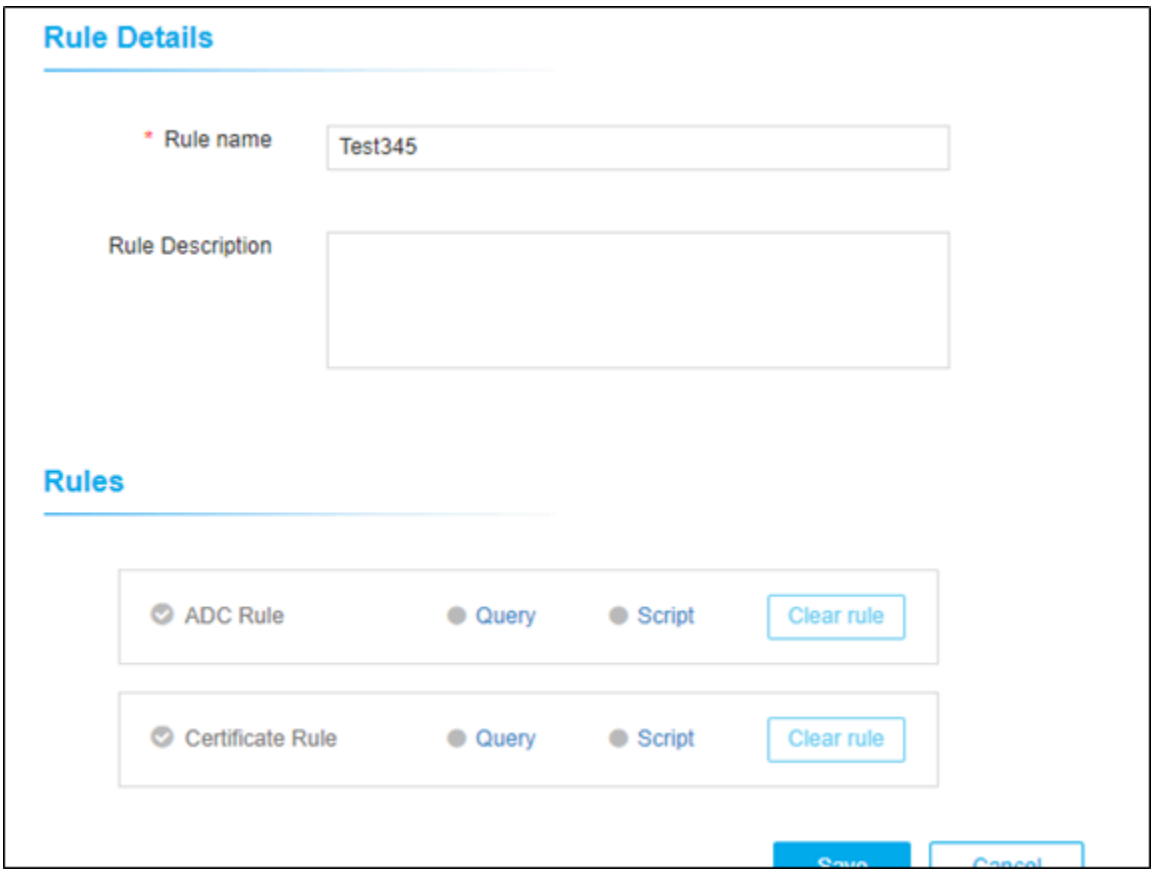



5. Click **Save**.
6. Saved rules will be displayed in the Rules tab. Go to the **Rules** tab by clicking on **Resource** in the breadcrumb.
7. Rule Summary details (Rule Name, Description, Rule Outcome) displayed in the Rule Inventory table.
8. Enable the rule by clicking on the respective status icon for the rule to be actively running.

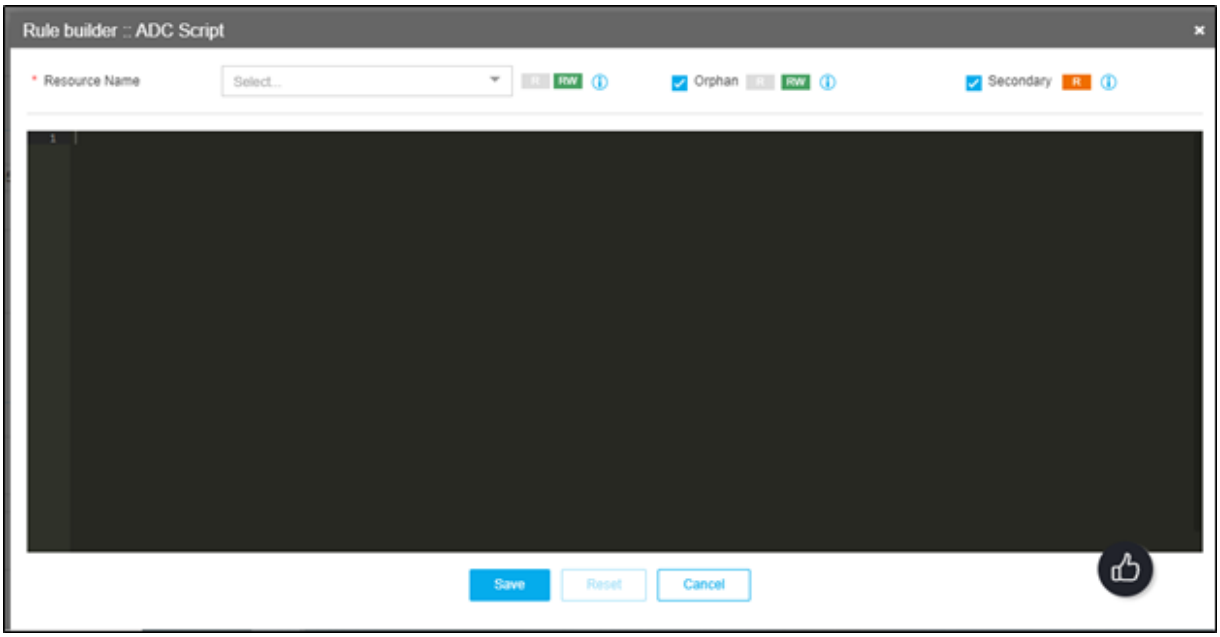
## Create an RBAC Rule to Tag ADC Objects/Certificates using a Script

To create an RBAC rule to tag resources using a Query:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. Click **Create Rule** from **Rules** tab.
4. In the Rule Name box, enter a name for the rule.
5. (Optional) In the Description box, enter additional information about the rule.
6. Under **Rules**, the option to configure ADC Rule and Certificate rule using Query/Script will be available.




7. Click **Script** hyperlink near the ADC/Certificate rule to configure a rule to dynamically tag ADC/ Certificates using Script.
8. Configure the details of the script, provide a resource name and assign required permissions.
9. For ADC Objects, Orphan and Secondary objects need to be assigned globally.
10. For Certificates, **Certificate Group Name** need to be provided.



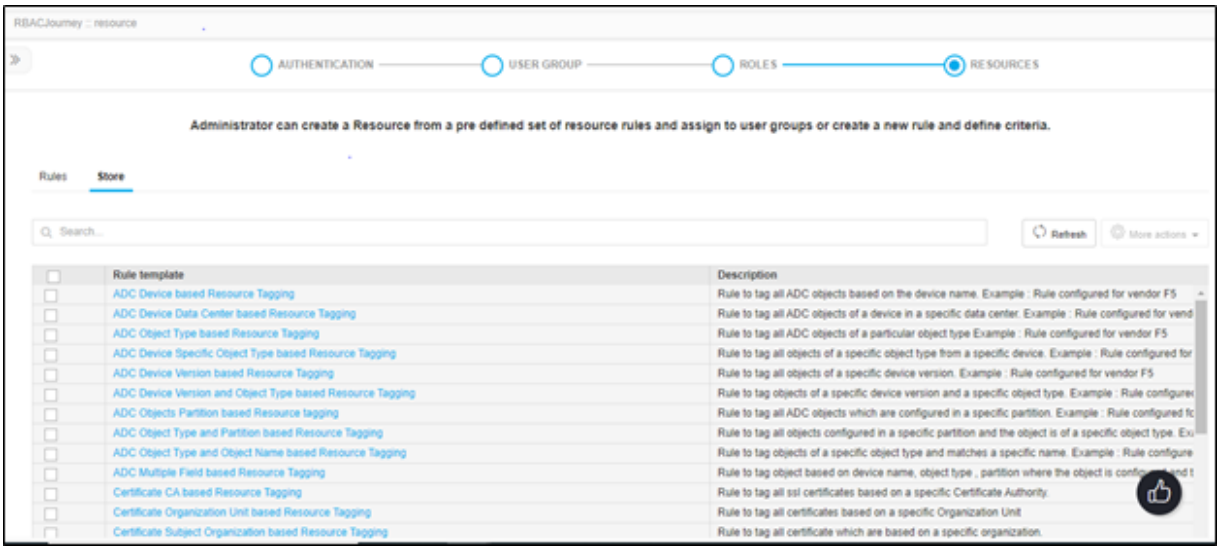

11. Click **Save**.
12. Saved rules will be displayed in the Rules tab. Go to the **Rules** tab by clicking on **Resource** in the breadcrumb.
13. Rule Summary details (Rule Name, Description, Rule Outcome) displayed in the **Rule Inventory** table.
14. Enable the rule by clicking on the respective status icon for the rule to be actively running.

## Clone a Rule

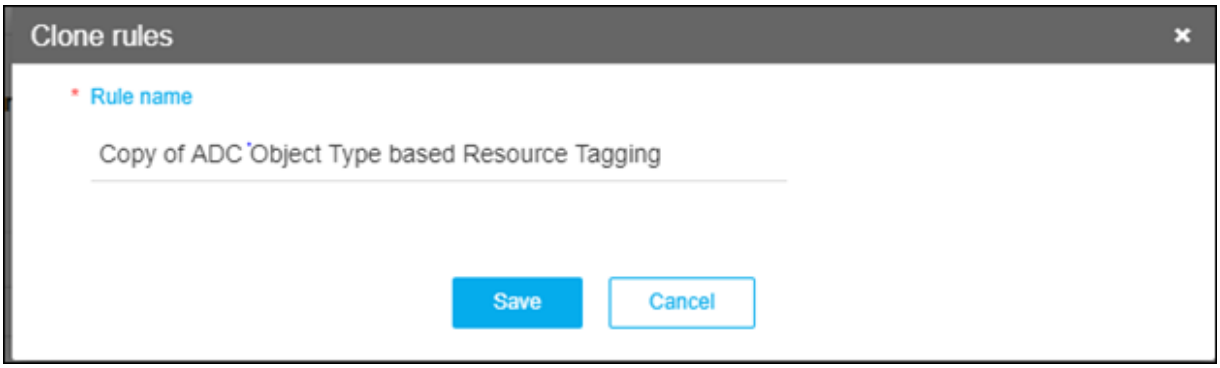
To clone a rule:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. Select the rule you want to clone either from **Rules** tab or from **Store** tab.

> **Note:** Store tab consists of predefined rule templates which can be viewed to understand possible resource tagging options.




4. From the More Actions dropdown, click Clone.
5. In the screen that appears, enter a Name for the cloned rule and click **Save**.




Rule details will be closed and will be opened in edit mode for any further modification on description/ rule conditions.

6. Once the rule is saved, Enable the rule by clicking on the respective status icon for the rule to be actively running in the rules inventory table.

## Delete a Rule

To delete one or more rules:

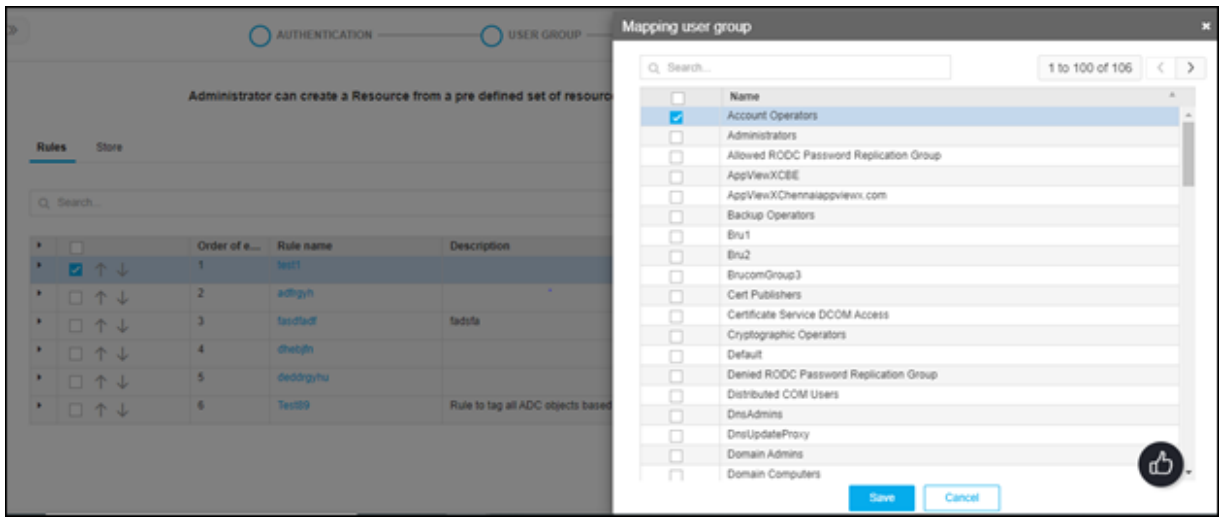
1. Click ☰ and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. Select the rule(s) you want to delete in the Rules tab.

4. From the **More Actions** dropdown, click **Delete**.
5. In the Confirmation dialog box that appears, click **Yes**.

## RBAC Rule Mapping to User groups to Dynamically Provide Access for Resources to User Groups

To map an RBAC rule to user groups:

1. Click and select **Account** > **User group** > **Quick Config**.
2. Navigate to **Resources** stage as part of the RBAC Configuration wizard flow.
3. On the rules list, select the checkbox beside the rule(s) you want to map to user groups based on rule outcome value.
4. Click on **Map User Group** option.
5. Select the required list of a user group(s) to be mapped for the selected rule(s) in the **Map User Group** pop up.
6. Click **Save**.
   The saved list of user groups will be displayed as a hyperlink in the rule inventory for each respective rule.




## Managing Order of Execution and Short Circuit Configuration for Rules

1. For managing the order of rule execution to avoid conflicts across multiple rules matching similar conditions and tag to expected resources, in the rule inventory table, click and hold a rule name and drag it up or down to change the order of execution of rules in use in the system.
   The order will be automatically saved.

2. Else, click up or down arrow beside each rule name to update rule execution order.
   - Order of execution needs to be maintained by the user only to manage certificates tagged to expected certificate groups configured part of a rule, as certificates can’t be part of multiple certificate groups
   - Based on the order of execution and matching rule condition, certificates will be only tagged to the certificate group at the top of rule execution order even though other RBAC rules down the order have a matching condition.
   - Order of execution also needs to be maintained by the user for ADC objects tagging to a specific resource only when Short circuit option is turned on for ADC
     - By default, a short circuit will be turned off for ADC as ADC objects can be tagged to multiple resources. There is no such restriction for ADC as it is existing for a certificate tagging. For certificates, a short circuit will always be turned on and can’t be changed by the user.
     - To enable a short circuit for ADC, click **More** icon under the **Rules Inventory>> Enable Short Circuit for ADC**.

# Chapter 9: System Module

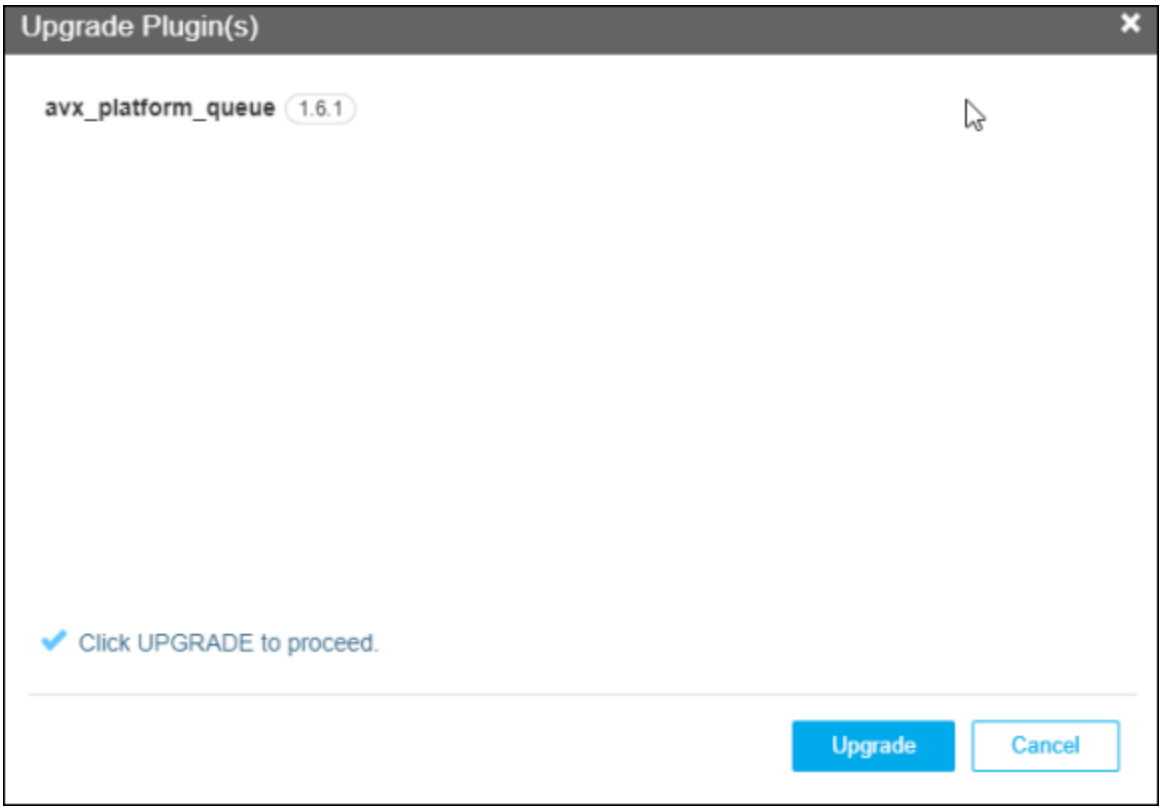


## Plugins Manager (Beta)

Users can manage plugins in the **System** module.

1. Click  and select **System** > **Plugins Manager**.
2. In the Manage Plugins page, you will see two sections: **Installed** and **Available**. You will be directed to the Installed section by default.
3. You can click **Available** to view the list of plugins that are not installed currently, but offered by AppViewX.
4. In the section you will find a list of plugins with details such as Plugin Name, Description, Running Version, and Latest Version. There is also a search bar to search for a particular plugin.
5. To view the changelog click  near the respective plugin.
6. To upgrade the plugin to the latest version, you can click 

near the respective plugin.
7. Click **Upgrade** again when the following screen appears:




8. Click Refresh to refresh the current list of plugins.

## Performing Actions

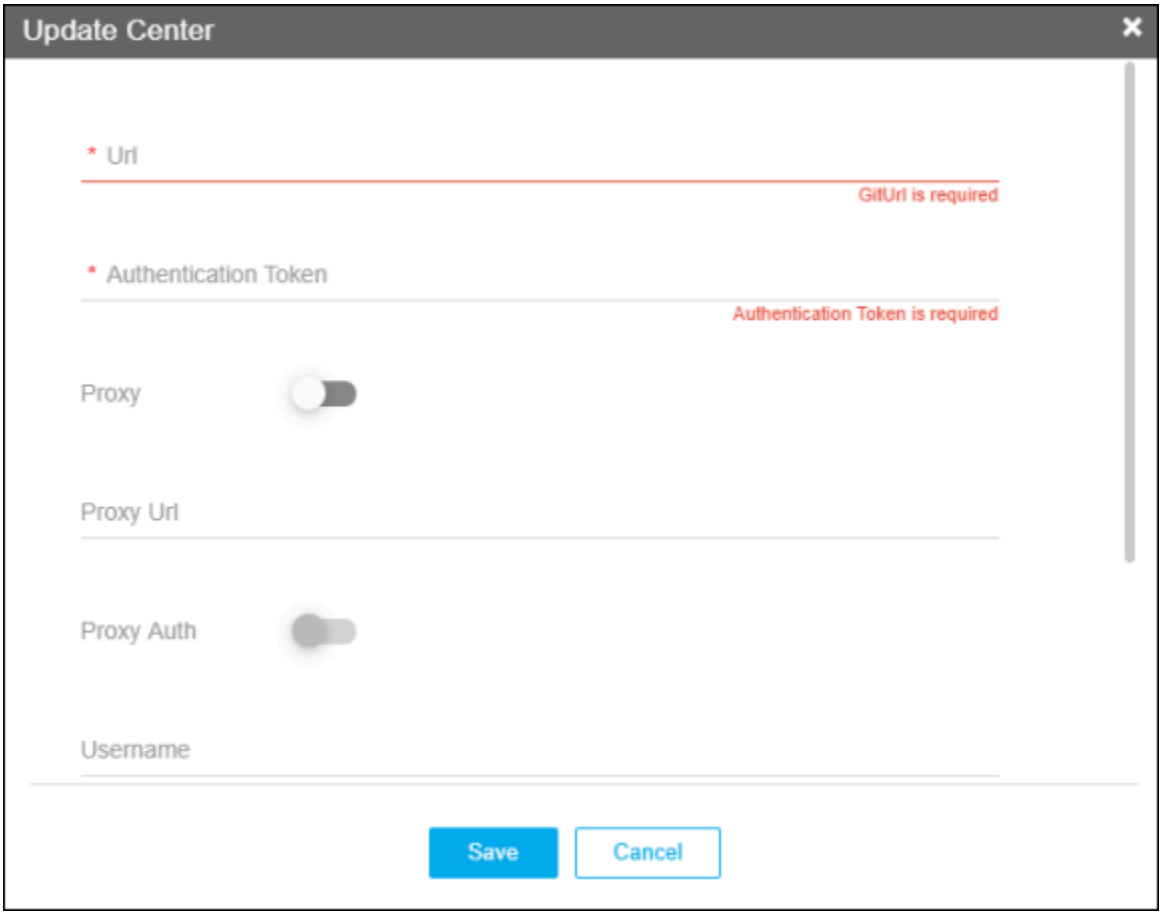
To perform operations on one or multiple plugins, select the checkbox before respective plugins, and then click Actions. Now you can upgrade or download the selected plugins.

## Upload Plugin

1. To upload a plugin from your local machine select Upload Plugin in the top right corner of the screen.
2. You can select a plugin in the **TAR.GZ*** format and then click **Upload**.

# Settings

1. To view the Update Center you can click the **Settings** icon in the top right corner of the screen. The following screen appears:




2. Enter the URL and the Authentication Token after receiving the details from the AppViewX support. These details are mandatory inputs.
3. You can enable Proxy if you do not have a direct internet connection. If that proxy server requires authentication, enable the Proxy Authentication. You can enter the credentials in the respective fields and click **Save**.
4. You also have the option to select the **Sync Time** which is the interval where AppViewX checks the existing list of plugins for the latest version available. You can choose between **daily, weekly, monthly**, and **yearly**.

# Platform Upgrade (Beta)

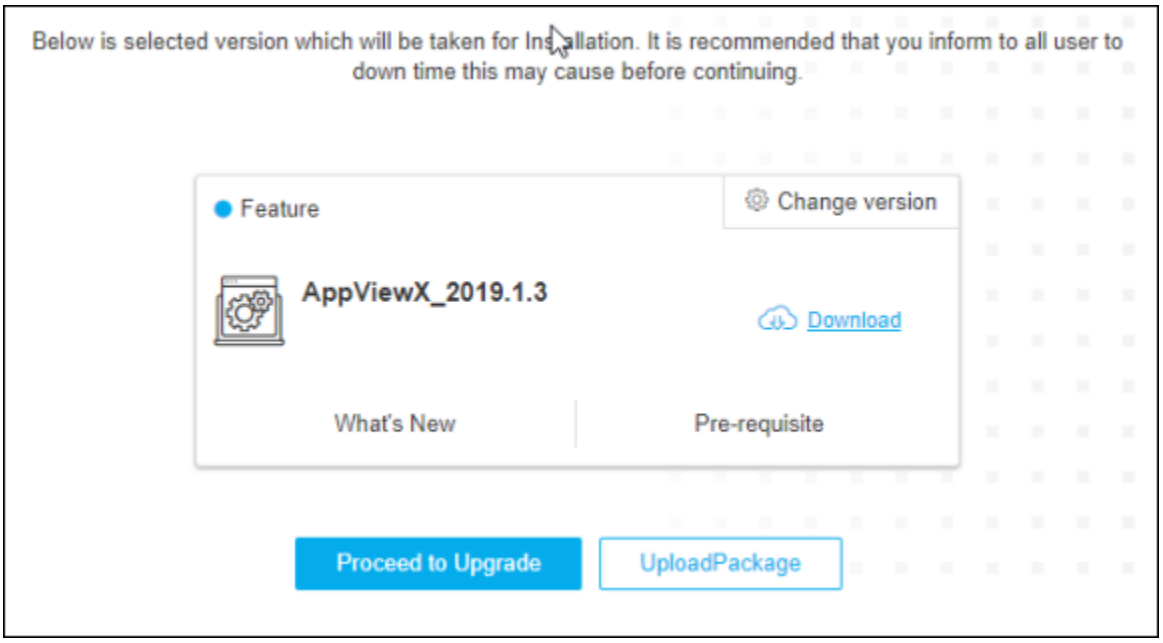
You can now update your current product version using this feature. To do so complete the following steps:

1. Click ☰ and select **Systems** > **System Update**.
   You will be directed to the following screen:


2. In the left pane, you can see the current version of the product that you are running.
3. In the right pane, you can see the available list of incremental upgrades for the AppViewX product.

> **Note:** Please note that you can only upgrade to a higher version of the product. You will not be able to downgrade to a lower version.

4. If you are already running the latest version of AppViewX, you will see this message on the right pane: 'No latest version available'.
5. If you are running an older version of AppViewX, then you will see the following screen on the right pane:




6. Here, you will find the latest AppViewX version. If you want to upgrade to an intermediate version (Versions that have been released during the timeline between your current release and the latest release) you can select **Change Version** and select the respective version that you want to upgrade to.
7. To know what are new features available in the particular release click **What's New**.
8. To know about the prerequisites needed to perform the upgrade click **Pre-requisite**.
9. If you have any Internet limitations for you to proceed to the upgrade directly, you can also download the update file locally to your machine and then upgrade to that release. To do so, complete the following steps:
   - Click **Download**
   - Once you have downloaded the file locally, click **Upload Package.**
   - Select the file on your local machine and then click **Install**
   - Now the upgrade process will begin. You can track the progress on the window.
   - You can view the step-wise details.
   - You will see the following screen once the process is complete:
   - Once you click **Launch** you will be redirected to the AppViewX login page.

# Chapter 10: Logging



## Logging Module

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
- Self-audit
- Certificate
- ADC
- AppViewX
- Syslog - AppViewX communicates with the device or KAFKA server (to enable KAFKA, refer to the **AppViewX 2019.4.0 Administrator Guide**), receives the syslogs, and processes the changes based on the configured interval. This will provide a near real-time update for the ADC device objects (F5, A10, AVI, and Citrix vendors), Firewall (Fortinet, Fortigate, Checkpoint, PaloAlto, Panorama, and Cisco) and WAF subsystems. Based on the Syslog updates, the CDU process is initiated and the configuration drift of an object for a configured interval will be displayed as a report in the Inframaps.
- SSH

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. Click and select **Logging**.
   The Logging screen opens, displaying all logs by default.
2. Click the tab that corresponds to the type of log you want to view.
3. On the log screen, view all details for a log by hovering your cursor over each column of data or click for the log you want to view. The table row expands to display all details for the log.

## Configure Logging for ADC Object Types

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.

To configure logging for a specific ADC object type:

1. Click and select **Logging**.
2. Click 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.
5. In the **Object Type** field, select the object that you want to generate a log report for.
6. In the **Available** field, click » beside each object you want to include in the log report.
7. In the Repeats field, select how often you want the log report to be generated: Daily, Weekly, or Monthly.
8. From the **Log severity** dropdown list, select one of the following:
   - Critical
   - Fatal
   - Major
   - Minor
   - Notification
   - This is to let the user know the severity of the log reports that have been sent.
9. In the **Email** field, enter email addresses of users receiving the log report.
10. (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.
11. Click **Add** to add the log report generation task to the table at the bottom of the screen.

# Export a Log

When exporting logs in AppViewX, you can export all of the logs of a given type-for example, all Config files or all Audit files-or you can search for specific logs or filter the default log list using the Date Range and Log Detail fields and then export only the logs that remain.

To export a logging report:

1. Click  and select **Logging**.
2. At the top of the Logging screen, click the tab for the type of logs you want to export: All, Audit, Self Audit, and so on.
3. (Optional) Run a search for specific logs or filter the default list using the Date Range and/or Log Detail fields in the Search bar.
4. Click  in the Command bar.
5. On the screen that opens, select the location where you want the log file to go, then click Save.
   The log report is then downloaded as a tar.gz file.

# Chapter 11: Alert



## Alert Module

Alerts identify complications that occur within the application. It can be sent at a predetermined date and time using an Email/SNMP configuration. In AppViewX, alerts are 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.

## Search for an Alert

The search feature within the Alert module allows you to run a basic search of all columns of data for any alert. Wildcards and the Boolean operators AND and OR are not supported. You can, however, create a search using the NOT operator to find all results that do not contain a word, phrase, or number. For

example, if you create an Alert Detail search and enter NOT memory in the search field, none of the alerts that appear in the results list will contain the word memory in their description.

To search for an item:

1. Click and select **Alert**.
2. On the top of the Alert screen, click the tab that corresponds to the type of alert you want to search for or leave the default All tab open to search through all alerts in the system.
3. In the **Search** field, enter a word, phrase, or number combination that appears in the Devices, Applications, or Detail column for the alert you are searching for.
4. (Optional) Use the calendar filter to restrict the date range of the alert to specific start and end dates, times, and minutes.
5. Click **Enter** on your keyboard to run the search.
6. In the results list, locate the alert you want to review, then click in the first column to expand the **Detail Column** to show all details.

## Create an ADC Alert

To create an ADC alert:

1. Click and select **Alert**.
2. On the **Alert** screen, click 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 » 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 +, 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:
    a. Select the **Email Configuration** checkbox.
    b. In the **Email Address** field, enter email addresses to send the alert. Use commas to separate the addresses.
    c. 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:

a. Enter the **Destination IP** for the alert.
b. Select the **Version** of SNMP you want to use: V1 or V2.
c. Enter the port the alert that should be used for the alert.
d. 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 Certificate Validation Alert

To create a certificate validation alert:

1. Click  and select **Alert**.
2. On the **Alert** screen, click  on the top.
3. On the Settings screen, click the **Certificate** tab.
4. Enter a name for the certificate alert.
5. Select the **Severity** of the alert: Critical, Major, or Notification.
6. In the **Alert Message** field, enter the text that users see when the alert appears on the screen.
7. Select the **Vendor** whose device or application you are creating an alert for.
8. In the **Event Type** field, select **Certificate Validation Alert**.
9. In the **Device Name** field, select the device associated with the certificate you are creating an alert for.
10. In the **Application** field, select the application associated with the certificate you are creating an alert for.
11. Select the **Execute Script** checkbox.
12. In the **Execute Script** dropdown list, select the script to trigger the alert.
13. To create a script, click  .
14. 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:

a. Select the **Email Configuration** checkbox.
b. In the **Email Address** field, enter email addresses to send the alert to. Use commas to separate the addresses.
c. In the **Subject** field, leave the default text or enter the text that briefly describes the alert the user is receiving.

15. To use the **Simple Network Management Protocol** (SNMP) to send the alert, complete the following steps:
    a. Enter the **Destination IP** for the alert.
    b. Select the **Version** of SNMP you want to use: V1 or V2.
    c. Enter the port the alert that should be used for the alert.
    d. 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.
16. Click **Add** to create the alert. It then appears at the bottom of the screen and on the **Certificate** tab within the Alert module.

## Create a Certificate Expiry Alert

Certificate expiry alerts are sent to designated recipients for all certificates that are set to expire on the date specified on the Settings: Certificate expiry alert screen.

To create a certificate expiry alert:

1. Click  and select **Alert**.
2. On the Alert screen, click  on the top.
3. On the Settings screen, click the **Certificate** tab.
4. Enter a name for the certificate alert.
5. Select **Critical** as the severity of the alert.
6. You can skip the **Alert Message** and **Vendor** field.
7. In the **Event Type** field, select **Certificate Expiry Alert**.
8. In the **Expires in** (days) field, enter the number of days before a certificate expires. An alert will be sent out.
9. 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:

a. Select the **Email Configuration** checkbox.
b. In the **Email Address** field, enter email addresses you want to send the alert to. Use commas to separate the addresses.
c. In the **Subject** field, leave the default text or enter the text that briefly describes the alert the user is receiving.

10. To use the **Simple Network Management Protocol** (SNMP) to send the alert, complete the following steps:
    a. Enter the **Destination IP** for the alert.
    b. Select the **Version** of SNMP you want to use: V1 or V2.
    c. Enter the port the alert that should be used for the alert.
11. 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.
12. Click **Add** to create the alert. It then appears at the bottom of the screen and on the **Certificate** tab within the Alert module.

## Create a Certificate Sync Alert

To create a certificate sync alert:

1. Click  and select **Alert**.
2. On the Alert screen, click  on the top.
3. On the Settings screen, click the **Certificate** tab.
4. Enter a name for the certificate alert.
5. Select the **Severity** of the alert: Critical, Major or Notification.
6. In the **Alert Message** field, enter the text that users see when the alert appears on the screen.
7. Select the **Vendor** whose device or application you are creating an alert for.
8. In the **Event Type** field, select **Certificate Sync Alert**.
9. In the **Device Name** field, select the device associated with the certificate you are creating an alert for.
10. In the **Application** field, select the application associated with the certificate you are creating an alert for.
11. Select the **Execute Script** checkbox.
12. In the **Execute Script** dropdown list, select the script to trigger the alert. To create a script, click  .
13. 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:

a. Select the **Email Configuration** checkbox.
b. In the **Email Address** field, enter email addresses to send the alert to. Use commas to separate the addresses.
c. In the **Subject** field, leave the default text or enter the text that briefly describes the alert the user is receiving.

14. To use the **Simple Network Management Protocol** (SNMP) to send the alert, complete the following steps:
    a. Enter the **Destination IP** for the alert.
    b. Select the **Version** of SNMP you want to use: V1 or V2.
    c. Enter the port the alert that should be used for the alert.
    d. 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.
15. Click **Add** to create the alert. It then appears at the bottom of the screen and on the **Certificate** tab within the Alert module.

## Create a Syslog Alert

AppViewX subscribes to all device-level alerts, where it acts as a syslog listener. Logs of any device added in AppViewX can be viewed as syslogs. However, devices tend to generate a huge amount of data, a **Syslog Alert** is a convenient way to notify about the specific syslog information that is of importance to you.

To create a syslog alert:

1. Click  and select **Alert**.
2. On the Alert screen, click  on the top.
3. On the Settings screen, click the **Certificate** tab.
4. On the Settings screen that opens, click the **Syslog** tab.
5. In the **Alert Name** box, enter a name for the alert.
6. In the **Alert Description** field, enter a description about the alert.
7. Select the **Severity** of the alert: Critical, Fatal, Major, Minor or Notification.

> **Note:** Instead of adding devices manually, 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.

8. In the **Filter** dropdown field, ADC is selected by default.
9. Select the **Vendor** for the ADC: **A10**, **Citrix**, or **F5**
10. Select the **Object Type** for the ADC: **FQDN**, **ServiceIP**, **VirtualService**, **ServiceGroup**, **Server**, **VirtualServer**, or D**evice**
11. In the **Available** column, a list of all available ADC objects or devices is displayed based on the object type and vendor selected.
12. Click » beside each object or device to add them to the **Assigned** column.
13. In the **Regex** field, you can enter single or multiple regex patterns/strings in the single text box using commas. The comma is considered as **Boolean AND** operator.
14. Click + to enter multiple regex patterns/strings in the multiple text box. The **Add** button is considered as **Boolean OR** operator.
15. To remove the regex patterns, click 🗑 beside the respective text box.
16. Click the **Execute Workflow** checkbox and from the dropdown list, select the workflow to trigger.
17. (Optional) In the **Metadata** section, enter a key and its associated value in respective fields. This is to define a condition based on which the workflow will be triggered.
18. To remove the key-value pairs, click 🗑 beside the respective text box.
19. 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:
    a. Select the **Email Configuration** checkbox.
    b. In the **Email Address** field, enter email addresses to send the alert. Use commas to separate the addresses.
    c. 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.
20. To use the **Simple Network Management Protocol** (SNMP) to send the alert, complete the following steps:
    a. Enter the **Destination IP** for the alert.
    b. Select the **Version** of SNMP you want to use: V1 or V2.
    c. Enter the port the alert that should be used for the alert.
    d. 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.
21. Click **Add** to save the alert to the AppViewX system.

## Create an SSH Alert

To create an SSH alert:

1. Click and select **Alert**.
2. On the Alert screen, click on the top.
3. On the Settings screen that opens, click the SSH tab.
4. In the **Alert Name** box, enter a name for the alert.
5. 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.
6. In the **Event type** box, select from the following event types:
   - SSH key expiry alert
   - Compliance alert
   - SSH key Push failure alert
   - SSH Discovery failure alert
   - SSH key deletion alert
   - SSH Host Modify/Delete alert
7. (SSH key expiry alerts only) In the **Expires in (days)** field, enter the total number of days until the key expires. The AppViewX system will trigger an alert message when this value is reached.
8. (Compliance alerts, SSH key Push failure alerts, and SSH key deletion alerts) In the **SSH Key Group** field, enter the key group you want to use as the basis for the alert.
9. (SSH key Push failure alerts and SSH key deletion alerts) In the **Key Alert Criterion** field, select whether you want to include logged-in user keys or all user keys in the alert.
10. (SSH Host Modify/Delete alert only) In the **SSH Host Group** field, enter the host group you want to use as the basis for the alert.
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:
    a. Select the **Email Configuration** checkbox.
    b. In the **Email Address** field, enter email addresses to send the alert. Use commas to separate the addresses.
    c. 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:

a. Enter the **Destination IP** for the alert.
b. Select the **Version** of SNMP you want to use: V1 or V2.
c. Enter the port the alert that should be used for the alert.
d. 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.

## Create an AppViewX Alert

To create an AppViewX alert:

1. Click  and select **Alert**.
2. On the Alert screen, click  on the top.
3. On the Settings screen that opens, click the **AppViewX** tab if it is not already open.
4. In the **Alert Name** box, enter a name for the alert.
5. 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 major priorities 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.
6. In the **Event type** box, select from the following event types:
   - Infrastructure
   - Application Discovery
7. If you want to use email to send out the alert, SMTP must first 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:
   a. Select the Email configuration checkbox.
   b. In the Email address field, enter each email address you want to send the alert to. Use commas to separate the addresses.
   c. 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.
8. Click **Add** to save the alert to the AppViewX system.

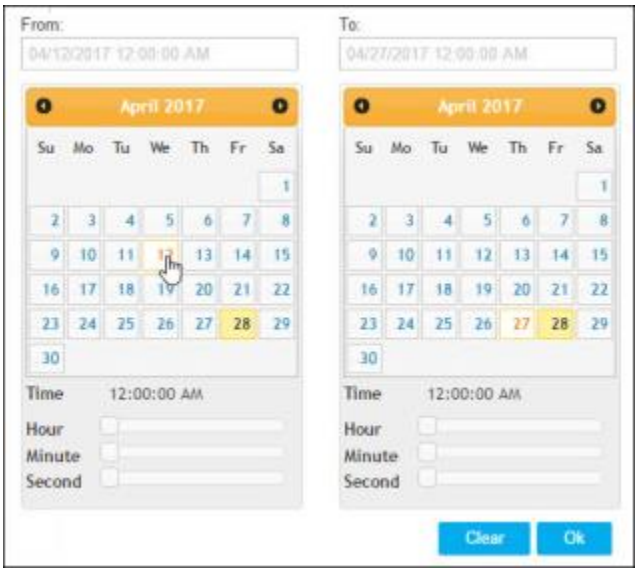
# Filter the Alert List

To filter the alert list that appears by default or as a result of a search:

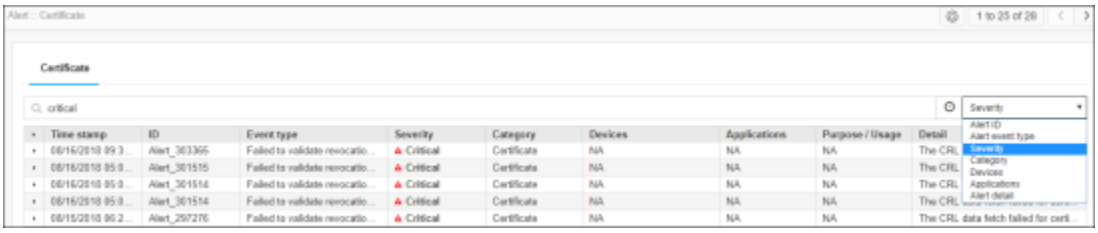
1. Click and select **Alert**.
   The Certificate alert tab appears.
2. Click one of the alert type tabs at the top of the screen to view only that kind of alert: certificate, SSH, AppViewX, or ADC.

> **Note:** The filter supports only one value at a time, so you cannot select **Severity** in the dropdown list and then enter Critical or Major in the search field. You must filter first by Critical, delete the value from the search field and click **Enter** to return to the complete results list, then enter the value **Major** in the search field and click Enter.

3. (Optional) Filter the updated alert list by date range by clicking and selecting the beginning and ending dates, hours, minutes, and seconds of the range you want to use. When you are done, click Ok to apply the filter.




4. (Optional) Filter the list by clicking the Alert detail dropdown menu at the end of the search bar and selecting one of the filter criteria. Entering the appropriate value in the search field, then press Enter on your keyboard. So, for example, if you selected Severity from the dropdown list, you would type a value such as Critical in the search field and then press Enter to apply the filter.

## Change the Settings for an Alert Type

The Alert module allows you to customize the settings for alerts in the system.

Fields in alert settings page differ based on the alert type, but the process for changing the settings is identical. To change the settings for an alert type, complete the following steps:

1. Click and select **Alert**.
2. On the Alert screen, click on the top.
3. Click on the tab that corresponds to the alert type to modify the settings.

> **Tip:** Click on **Reset** to reset to the original settings. Clicking on **Cancel** ignores all changes you made and closes the Settings screen, bringing you back to the Alert screen.

4. Make the required changes and click **Add** to update the settings.

# Chapter 12: Settings



## General Settings

The General settings component of the Settings module includes the following components used by all subsystems:

- Authentication
- License
- Log forwarding
- Login configuration
- SMTP
- Theme
- Proxy

- Authentication Settings
- License
- Log Forwarding
- Login Configuration
- SMTP
- Theme
- Proxy

## Authentication Settings

To configure authentication settings, navigate to **Menu** > **Settings** > **General** > **Authentication**.

## LDAP Authentication

**Note:** LDAP is selected by default or click LDAP on the top.

1. On the LDAP details page, under **General Information**, enter the Host and the Port number.
2. Click  to enable LDAP.
3. In the Upload Certificate field, click **Browse** to choose a certificate.
4. Enter the **Bind DN** and **Bind Password**.
5. Click the respective to enable authorization and LDAP sync.
6. Click **Test Connection**.
7. Under User Search, enter the User Search Base, Search Filter, and User Return Attribute.
8. Click Test Query.
9. Under **Group Search**, enter the Group Search Base, Group Search Filter, and Group Return Attribute.
10. Click **Test Query**.
11. Click **Save** to display the LDAP details or click **Reset** to reset the settings.

## TACAS Authentication

1. Click **TACACS** on the top.
2. On the TACACS details page, enter the Server Name, IP Address, and Port number.
3. Click **Test Connection**.
4. Enter Secret Key, Service, Protocol, and Authorization Attribute Name.
5. Click **Add** to add the settings or click Reset.
6. Added TACACS settings will be displayed on the left.
7. To fetch user group, delete, enable, and disable TACACS settings, select the settings from the list view and click the respective icon on the top right.

## RADIUS Authentication

1. Click **RADIUS** on the top.
2. On the RADIUS details page, enter the Server Name, Host, Shared Secret Key, Authentication Port, and Acceptance Port.
3. Select the **Authentication Mode** (PAP/ASCII, CHAP, MS-CHAPv2, EAP-MD5).

4. Click  to enable the Authorization.
5. In the **Authorization Via** field, choose Radius or LDAP.
6. Enter the **Vendor ID** and **Vendor Type**.
7. Click **Add** to add the settings or click Reset.
8. Added RADIUS settings will be displayed on the left.
9. To fetch user group, delete, enable, and disable RADIUS settings, select the settings from the list view and click the respective icon on the top right.

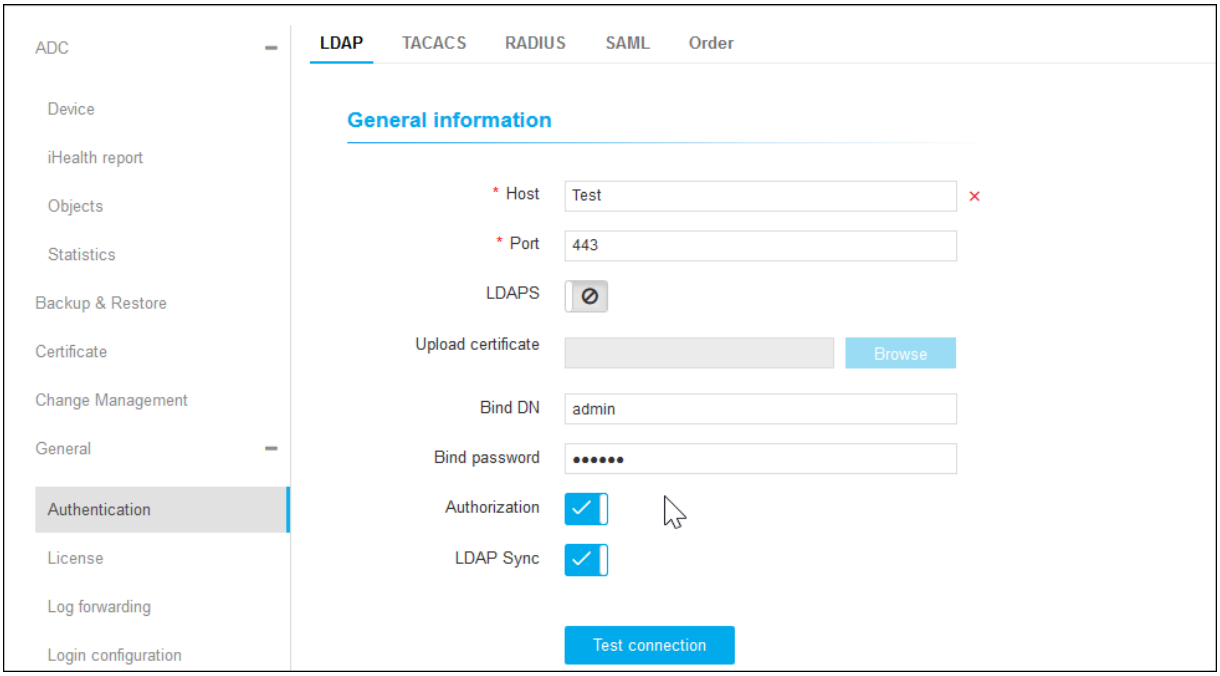
## SAML Authentication

1. Click **SAML** on the top.
2. On the SAML details page, under SSO Information, click  to enable SSO.
3. In the **MetaData** field, click **Browse** to import an identity provider (**IdP**) metadata by browsing to an XML file.
4. Enter the **Issuer URL** and **SSO URL**.
5. Click  to enable SLO.
6. Enter the **SLO URL**.
7. In the **Upload Certificate** field, click **Browse** to choose a certificate.
8. Click **Save**.

## ORDER Authentication

1. Click **ORDER** on the top.
2. On the ORDER details page, you can enable or disable LDAP, TACACS, RADIUS, and LOCAL by clicking respective icons.

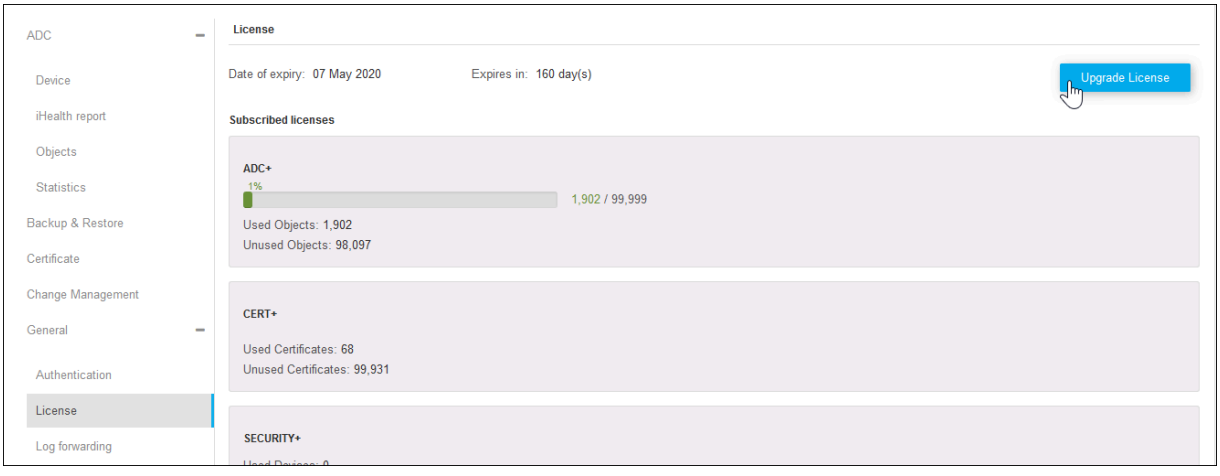
3. Click **Save**.




## License

To view the list of subscribed licenses and to upgrade a license:

1. Click ☰ and select **Settings** > **General** > **License**.
2. On the license details page, you can find the list of subscribed licenses with the expiry date.
3. Click **Upgrade License** on the top right.
4. On the Upgrade License window, click **Browse** to choose a license file.
5. Click **Upload**.




The user is notified with a pop-up warning whenever one of the following scenarios occurs:

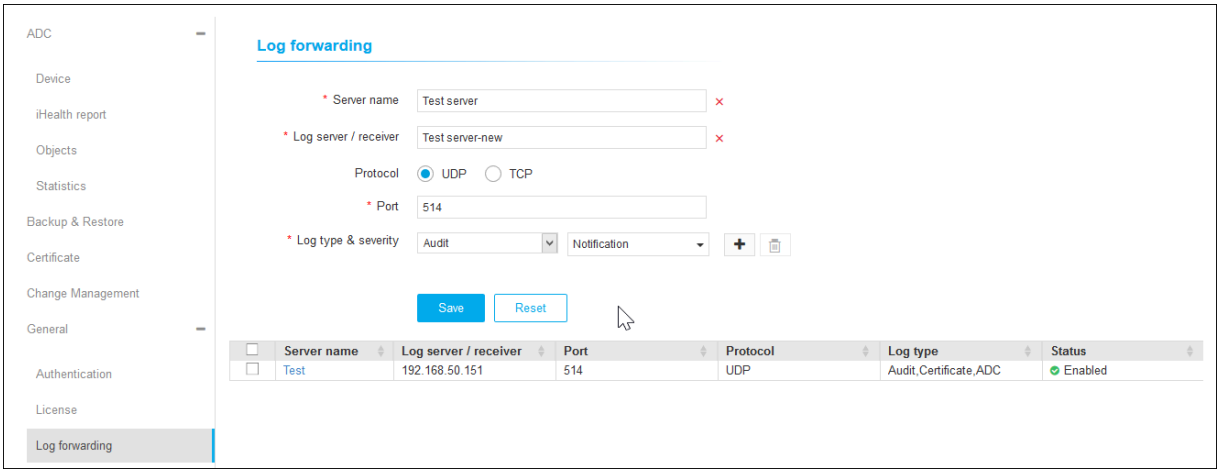
- The object, device or certificate count has reached or about to reach the license limit
- The subsystem license has expired or is about to expire

## Log Forwarding

To configure log forwarding details:

1. Click ☰ and select **Settings** > **General** > **Log Forwarding**.
2. On the Log Forwarding details page, enter the **Server Name** and **Log Server/Receiver**.
3. Choose the **UDP** or **TCP** protocol.
4. Enter the **Port** number.
5. Select the **Log Type** and **Severity** from the respective drop-down.

   To add multiple entries, click +.
6. Click **Save** to save the details or click **Reset** to reset the settings.
7. To delete, enable, and disable **Log Forwarding**, select the settings from the list view and click the respective icon on the top right.

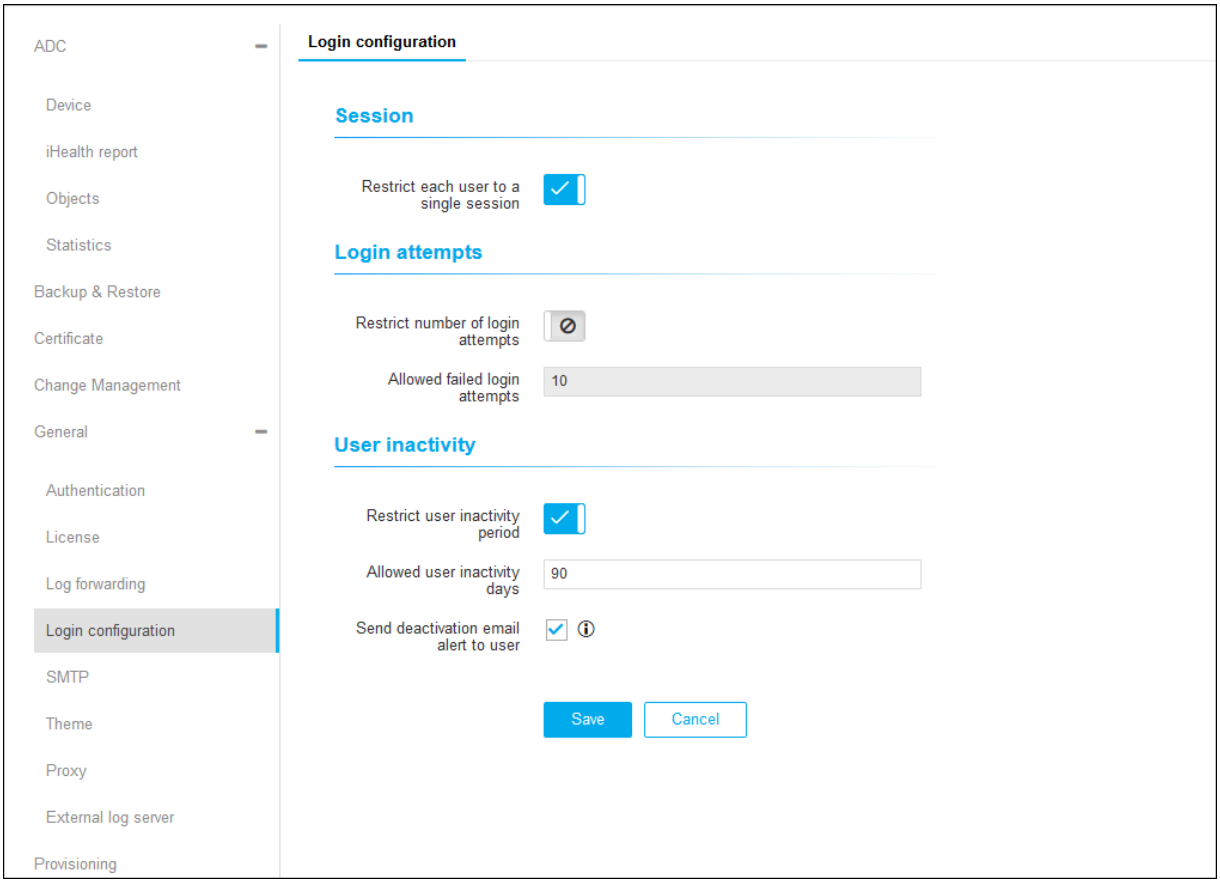



## Login Configuration

To configure login details:

1. Click ☰ and select **Settings** > **General** > **Login Configuration**.
2. On the Login Configuration details page, under Session, click ⊘ to enable **Restrict each User to a Single Session.**
3. Under Login Attempts, click ⊘ to enable **Restrict Number of Login Attempts**.
4. Enter a value for **Allowed Failed Login Attempts**.

5. Under User Inactivity, click  to enable **Restrict User Inactivity Period**.
6. Enter the **Allowed User Inactivity Days**.
7. Click the checkbox to enable **Send Deactivation Email Alert to User**.
8. Click **Save**.

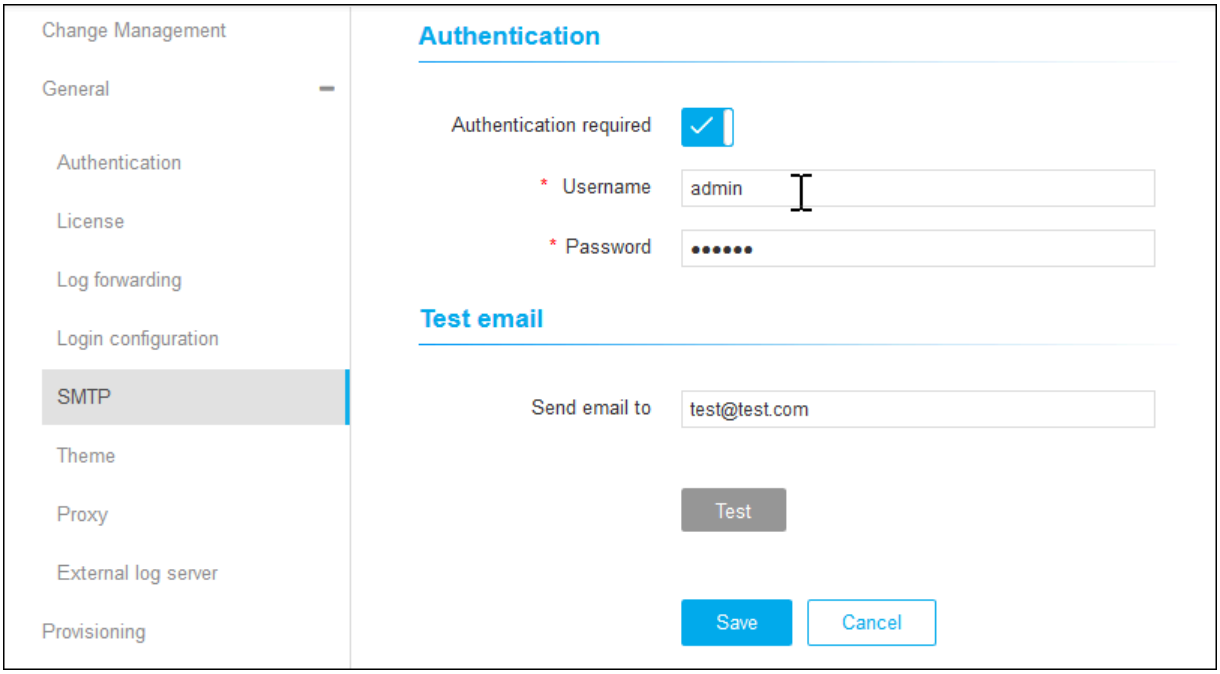



## SMTP

To configure SMT:

1. Click  and select **Settings** > **General** > **SMTP**.
2. On the SMTP details page, under SMTP Configuration, enter the SMTP host, port, and outgoing email address.
3. Click the disable icon to enable the **Email Box**.
4. Under Authentication, click  to enable **Authentication Required**.
5. Enter the username and password.
6. Under **Test Email**, enter the **Send Email to** address.
7. Click **Test** to check the connection.

8. Click **Save**.




## Theme

To configure theme settings, navigate to **Menu** > **Settings** > **General** > **Theme**.

## Logo

1. The **Logo** tab is selected by default or click Logo on the top.
2. Under Login, click  to **Enable Logo in the Login Screen and Header**.
3. In the **Upload Logo** section, choose an image to set the logo.
4. In the **Upload Favicon** section, choose an image to set the favicon.
5. Click **Save**.
6. Under Preview, you can view the uploaded logo and the favicon.

## Header

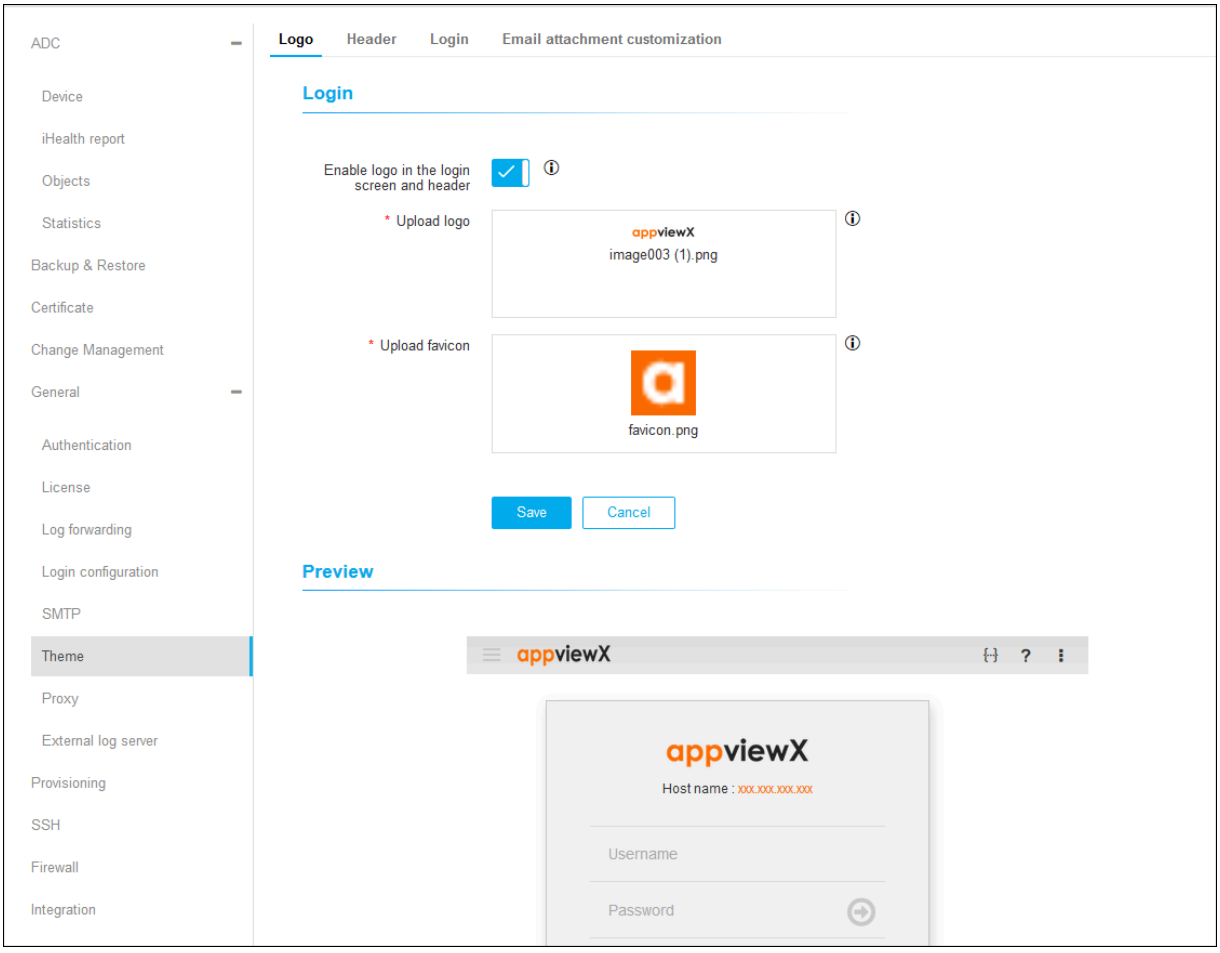
1. Click **Header** on the top.
2. Under Header Info, click  to enable **Display Label on Header**.
3. Under **Header Color**, select the header color, header icon, and font color.
4. Click **Save**.
5. Under Preview, you can view the header.

## Login

1. Click **Login** on the top.
2. Under **Login Credentials Entry Pane**, enter the background color and font color.
3. Under **Banner Image**, click  to **Enable Banner Image in Login Screen**.
4. In the **Upload Image** section, choose an image to set as a banner image.
5. Click **Save**.
6. Under Preview, you can view the login page.

## Email Attachment Customization

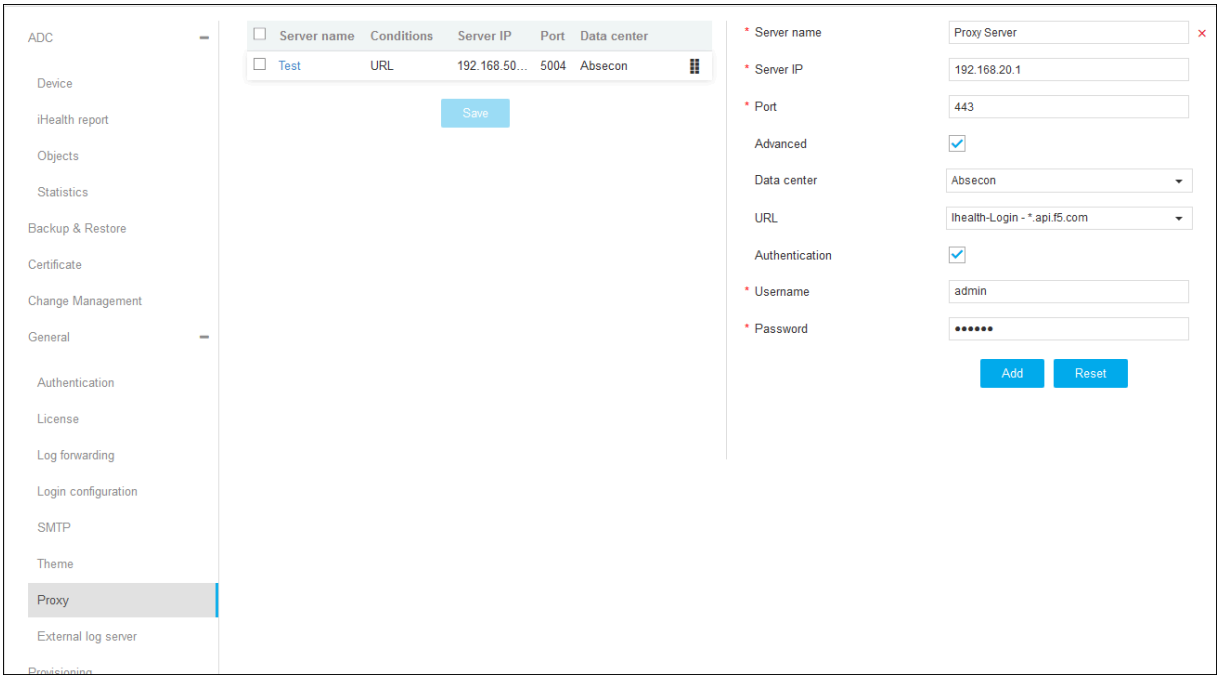
1. Click **Email Attachment Customization** on the top.
2. Under **PDF**, browse to choose a logo image.
3. Enter the **Document Title** and **Footer**.
4. Under **CSV**, enter the **Attachment File Size Limit**.
5. Click **Save**.



## Proxy

To configure proxy settings:

1. Click and select **Settings** > **General** > **Proxy**.
2. On the Proxy details page, enter the Server Name, Server IP, and Port number.
3. Enable the **Advanced** checkbox.
4. Select the **Data Center** and the **URL** from the respective dropdown.
5. Enable the **Authentication** checkbox if required.
6. Click **Add**. Added proxy settings will be displayed on the left.
7. To delete proxy settings, select a setting and click on the top right.




# ADC Settings

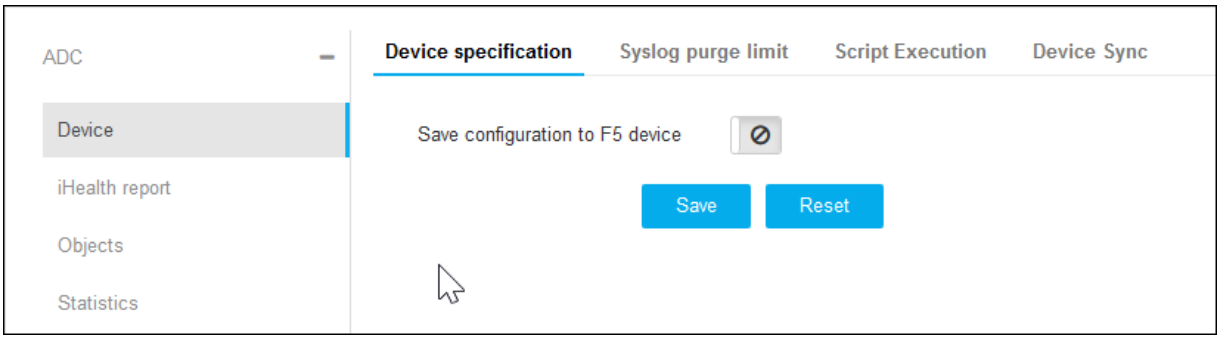
You can configure ADC settings by clicking and selecting **Settings** > **ADC**.

- Device
- iHealth Report
- Objects
- Statistics

## Device

To configure a device:

1. Click **Device** under the ADC menu.
2. On the Device details page, **Device Specification** is selected by default or click **Device Specification** on the top.
3. Click the disable icon to enable **Save Configuration to the device**.
4. Click **Save**.
5. Click **Syslog Purge Limit** on the top.
6. Enter the Syslog limit per device.
7. Click **Save**.
8. Click **Script Execution** on the top.
9. Enter the time out in minutes.
10. Click **Save**.
11. Click **Device Sync** on the top.
12. Select the time for **Config Fetch** and **HA-Sync** from the respective drop-down.
13. Click **Save**.

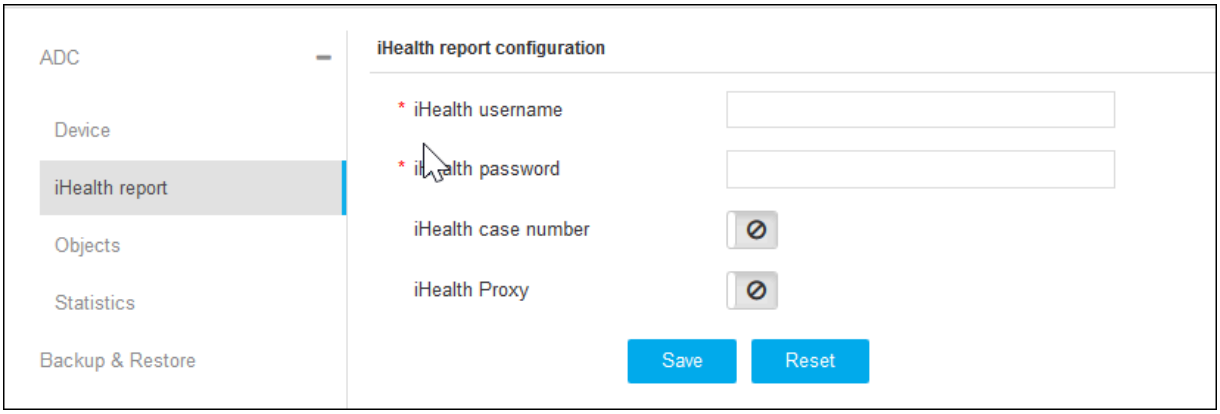



## iHealth Report

To configure iHealth report:

1. Click **iHealth Report** under the ADC menu.
2. On the **iHealth Report Configuration** page, enter the **iHealth username** and **password**.
3. Click  to enable **iHealth Case Number** and **iHealth Proxy**.

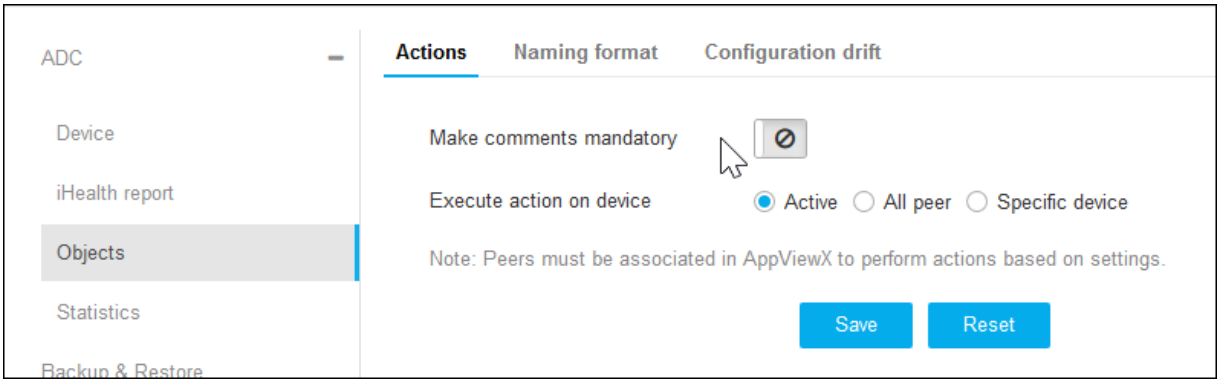
4. Click **Save**.




## Objects

To configure objects:

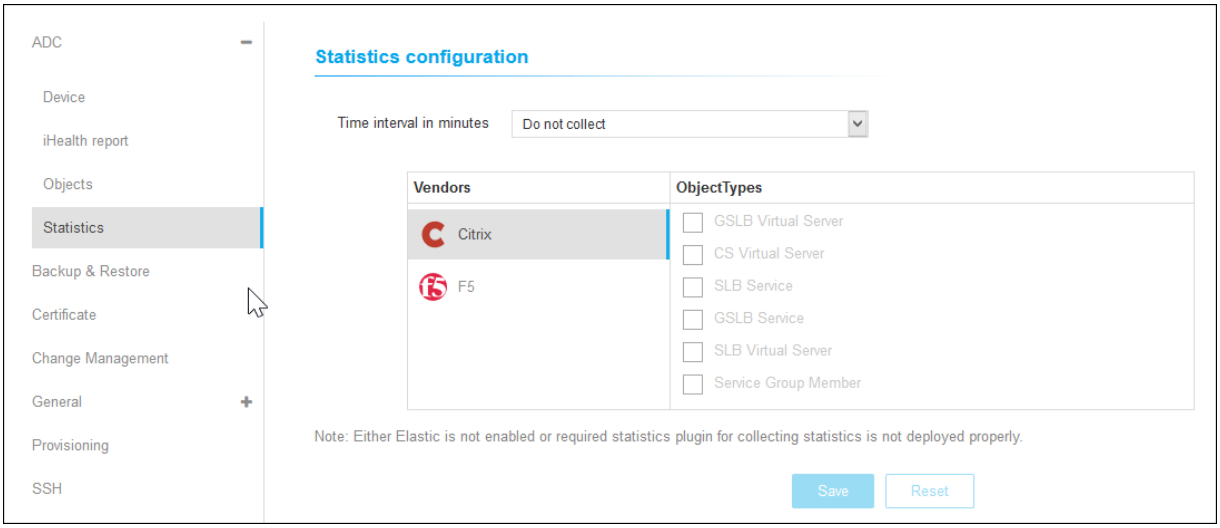
1. Click **Objects** under the ADC menu.
2. On the Objects details page, **Actions** are selected by default or click **Actions** on the top.
3. Click  to enable **Make Comments Mandatory**.
4. Select **Active** or **All Peer** or **Specific Device** radio buttons for **Execute Action on Device**.
5. Click **Save**.
6. Click **Naming Format** on the top.
7. On the **Display Name Format** page, you could find the display name format of vendors like A10, AVI, Akamai, AmazonELB, BigIQ, Cisco, Citrix, F5, HAProxy, Infoblox, and NginxPlus.
8. Select the options available for respective vendors.
9. Click **Save**.
10. Click **Configuration Drift** on the top.
11. Enter the number of days in **Store Configuration Drift for** field.
12. Click **Save**.



## Statistics

To configure statistics:

1. Click **Statistics** under the ADC menu.
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.
4. Click **Save**.




# Backup and Restore Settings

The **Backup & Restore** tab within the Settings module is where you can specify exactly how many archives you want to retain in the system.

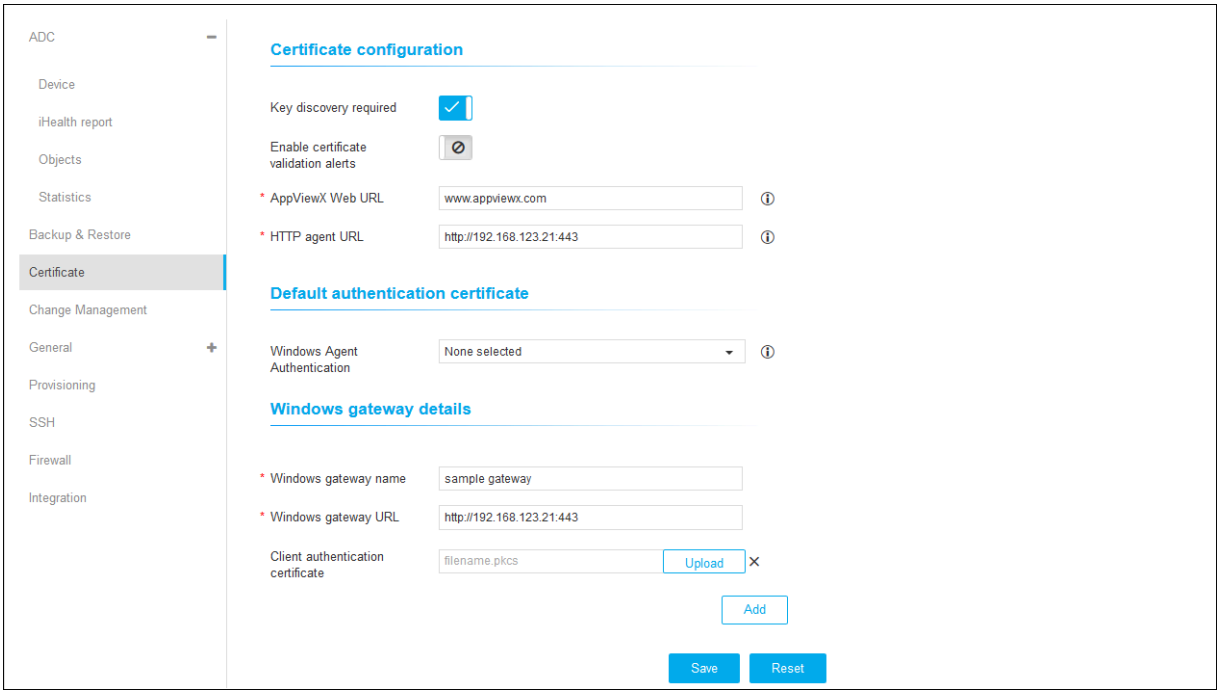
To set the backup limit:

1. Click ☰ and select **Settings**.
2. On the **Settings** screen, click the **Backup & Restore** tab.
3. In the Maximum number of archives field, enter the number of backups you want to retain at one time in the system.
4. Click **Save**.

# Certificate Settings

To configure certificate settings:

1. Click and select **Settings** > **Certificate**.
2. Under **Certificate Configuration**, enable **Key Discovery Required** and **Enable Certificate Validation Alerts**.
3. Enter the AppViewX Web URL and HTTP Agent URL.
4. Under **Default Authentication Certificate**, select **Windows Agent Authentication**.
5. Under Windows Gateway Details, enter a Windows Gateway Name and Windows Gateway URL.
6. Click **Upload** in the **Client Authentication Certificate** field and choose a file with **.pkcs** format.
7. Click **Add** to display the agent details.
8. Click **Save** to save the settings or click **Reset** to reset the settings.



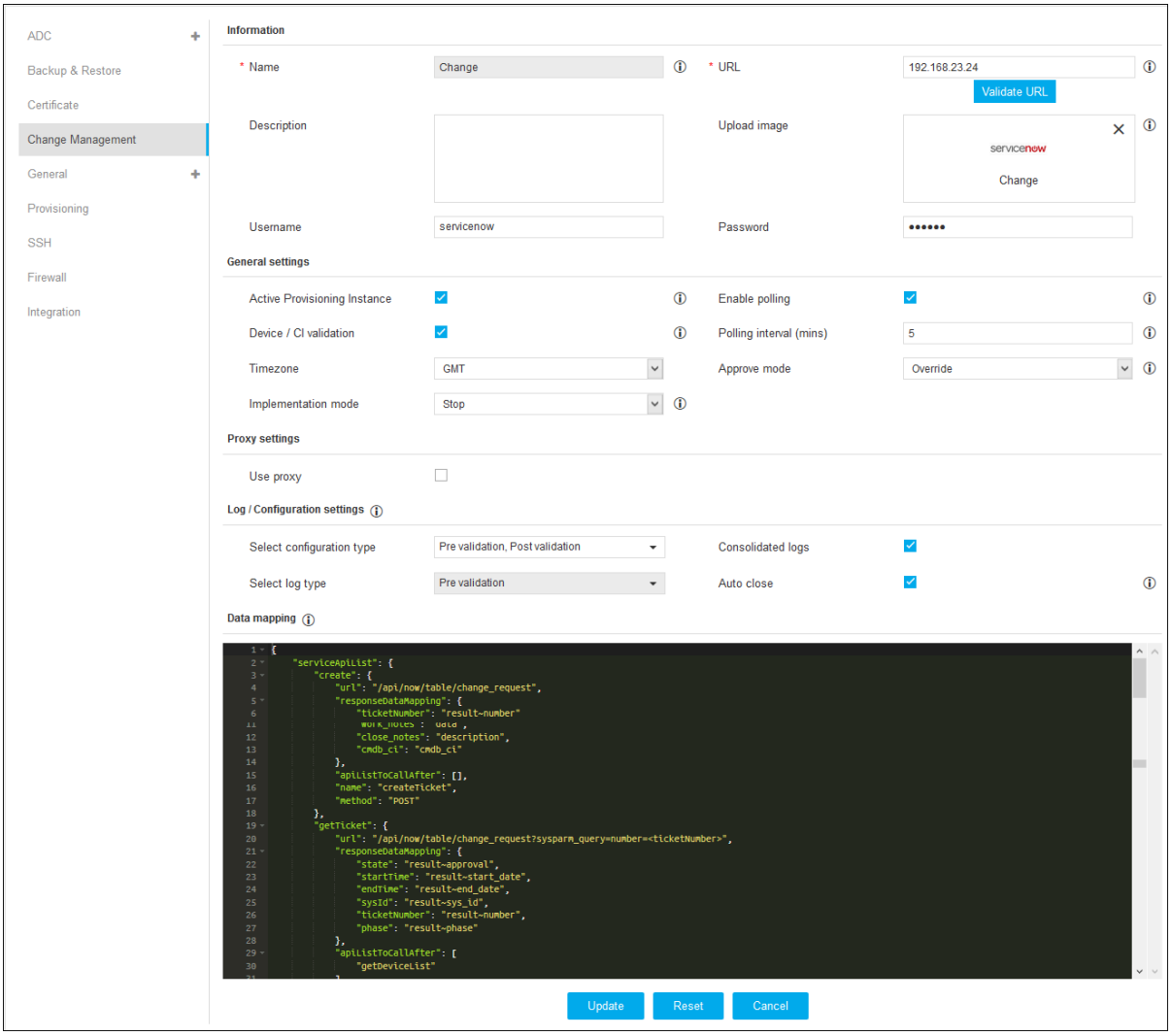

# Change Management

Change Management allows you to configure ITSM vendor instances. To configure ITSM vendor instances:

1. Click and select **Settings** > **Change Management**.
2. Click + icon on the top right.

3. On the **Vendor Configuration** details page, under Information, enter the name, URL, description, username, and password.
4. In the **Upload Image** section, choose a vendor image to upload.
5. Under General Settings, enable the respective checkboxes of **Active Provisioning Instance**, **Enable Polling** and **Device/CI Validation**.
6. Enter the **Polling Interval** time in minutes.
7. Select the time zone from the **Time Zone** drop-down.
8. Select Override or Stop from the **Approve Mode** drop-down.
9. Select Override or Stop from the **Implementation Mode** drop-down.
10. Under Proxy Settings, enable the **Use Proxy** checkbox.
11. Under Log/Configuration Settings, select the configuration type and log type.
12. Enable the respective checkboxes of **Consolidated Logs** and **Auto Close**.
13. Under Data Mapping, you can define ITSM configurations such as create ticket API, close ticket API, update API and data mapping between AppViewX and ITSM.

14. Click **Add** to add the vendor configuration details.



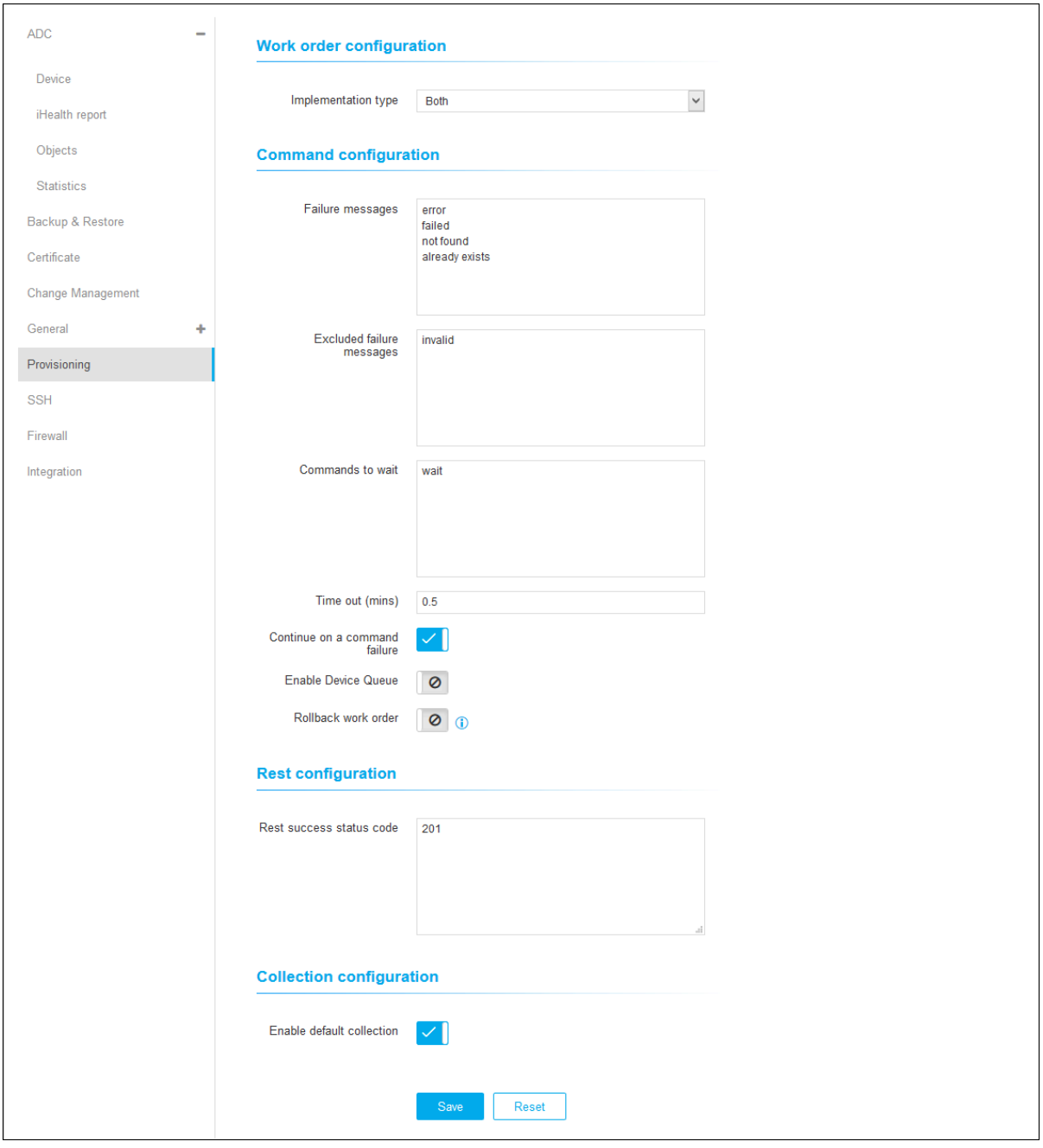

# Provisioning Settings

AppViewX Provisioning is a template-based request system that provides end-to-end application provisioning across Layer 4 - Layer 7 components. The Provisioning module allows you to specify the type of work order implementations you want users to be able to create provisioning for. Also to include command messages and REST configurations.

To configure provisioning settings:

1. Click ☰ and select **Settings** > **Provisioning**.
2. On the Provisioning details page, under **Work order Configuration**, choose the implementation type.

3. Under **Command Configuration**, enter the failure message, excluded failure messages, and command to wait.
4. Enter the **time out** in minutes.
5. Click  to enable **Continue on a Command Failure**, **Enable Device Queue,** and **Rollback Work order**.
6. Under **REST Configuration**, enter the REST Success Status Code.
7. Under **Collection Configuration**, click the disable icon to **Enable Default Collection**.
8. Click **Save**.



# SSH Settings

The SSH tab within the Settings module allows you to configure an LDAP directory server to push public keys to the LDAP directory user profile for SSH authentication and to set the IP type to cloud-based discovery.

- LDAP Configuration
- Cloud-Discovery Configuration
- Cyberark Web Authentication

## LDAP Configuration

To configure SSH authentication using LDAP:

1. Click and select **Settings**.
2. On the Settings screen, click the **SSH** tab.
3. The Publish SSH Public Keys on Directory field is set to "Disabled" by default. To enable it so that SSH public keys are pushed to the directory, click .
4. The LDAP field is set to **Enabled** by default, which allows public keys to be pushed to particular user accounts in the directory using a secure approach. To turn this feature off, click .

> **Note: Publish SSH Public Keys on Directory** must be enabled if you want to be able to associate, publish, and delete an LDAP connector for an SSH key.

5. In the Directory field, select from one of the following options:
   - Existing Auth. Directory Servers - This option retrieves existing LDAP servers' records from the Authentication tab.
   - New Directory Servers - This option adds new directory servers for pushing SSH public keys to the directory. If you select this option, four new fields appear on the screen. Complete the following sub-steps:
     - In the Host field, enter the host address of the Active Directory (AD) server.
       - For a single-domain Active Directory Domain Service (AD DS), the default port for LDAP is 389, while the default port for LDAP over SSL is 636.
     - In the Bind DN field, enter the full distinguished name (DN), including the common name (CN), of an Active Directory user account that has privileges to search for users.
     - For example: cn=manager,dc=sample,dc=com

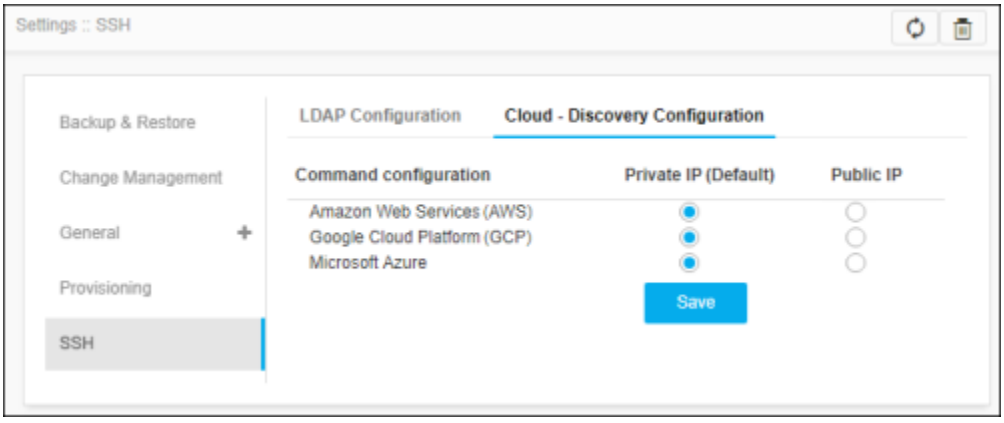
- The Bind DN user, such as the Administrator, is the username associated with the Bind DN user account. The Connector creates a corresponding user account as an administrative user in the Application Manager. You use the username for this account to log in to the Application Manager as an administrator. In AD DS, the Bind DN entry must be located in the same branch and below the Base DN.
- In the Bind Password field, enter the password associated with the Bind DN user account.
- In the Search base field, enter the name of the search base object, which defines the location in the directory from which the LDAP search begins.
- For example: ou=APPVIEWX,dc=sample,dc=com
- An LDAP search has the potential to retrieve information about all objects within a specific scope that have certain characteristics.

6. Select at least one of the directory servers from the collection list.
7. Click Add to add the LDAP configuration to the system.
8. Click Save to publish the public key file to the LDAP server user profile. If the LDAP server from the collection list is not selected, then publishing the public key will fail.

## Cloud-Discovery Configuration

To configure the IP type to be fetched for all managed devices:

**Note:** You cannot change the IP type while Amazon Web Services (AWS) instances exist in the inventory for the selected IP type.




1. Click the **Cloud - Discovery Configuration** sub-tab on the **SSH** tab.
2. In the **Amazon Web Services (AWS)** row, select any one of the following IP types:
   - **Private IP** - An IP address used within your private space. It is not directly exposed to the Internet.
   - **Public IP** - An IP address that can be accessed over the Internet.

3. Repeat Step 2 for the Google Cloud Platform (GCP) and Microsoft Azure rows.
4. Click **Save**.

## Cyberark Web Authentication

To configure the SSH settings using CyberArk:

1. Click the **CybeArk Web Authentication** sub-tab on the **SSH** tab.
2. If you want to publish SSH private keys on CyberArk, enable the option to do so.
3. The **Publish SSH Private Keys to CyberArk User** account field is set to "Disabled" by default. To enable it so that SSH private keys are push to the CyberArk user account, click  .

> **Note: Publish SSH private keys to CyberArk user account** must be enabled if you want to associate and publish (Push) private key to CyberArk user account and the client device within a single push workflow.

4. Once you have that option enabled, you will have access to the following options:
   - Enter the domain name and IP address in the **Domain/IP address** field.
   - Enter the port details in the **Port** field.
   - You can choose between HTTP and HTTPS in the **Methods** fields.
   - Enter the CyberArk web credentials username and password in the respective fields.
   - Click **Save**.

# Firewall Settings

The Firewall tab within the Settings module allows you to configure the level you want to use for profile association based on which the risk reports are generated in the Control Center module. For more details on how to generate a risk report, refer to the Configure Risk Settings section of this guide.

To configure firewall settings,

1. Click  and select **Settings**.
2. On the **Settings** screen, click the **Firewall** tab.
3. From the **Select level** dropdown list, select one of the following:

- **Policy**
- **Application**
- **Device**

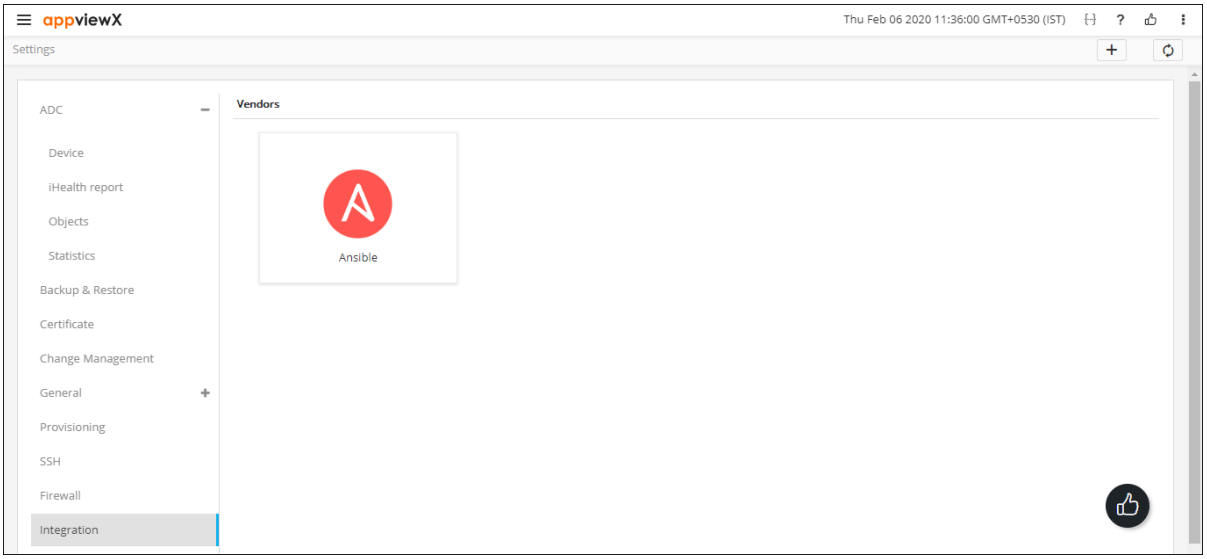
4. Click **Save**.

## Integration Settings

You can integrate with supported vendors to AppViewX.

To view or add a new vendor:

1. Click and select **Settings** > **Integration**.
   The following screen will be displayed.




2. To add a new vendor, click the + icon.
   You will be able to add a new vendor by entering the mandatory fields.

# Chapter 13: Insight



## ADC

The widgets in the ADC dashboard display device and application details based on the statistical data configured for a specific interval.

To view the widgets related to ADC:

1. Click  and select **Dashboard**.
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 **ADC**.
5. Although each report displays the data differently, the same set of data is used to generate each report. The following reports are segregated and displayed as widgets on the ADC screen:
   - **Device heat map** - A graphical representation of the health of the 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.
- **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 control center 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.
- **Number of Objects** - 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.
- **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.
- **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/Quater) you choose. This report helps users to scavenge unnecessary configurations of the device and manage configurations on the devices.

## App-centric Reports

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 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 VIP level traffic details for the period (day/week/month/quarter) you choose. It is used to determine the highest traffic served per VIP and all the traffic/connections served by the VIP in that application.

## Certificate Events and Actions List

A Certificate report displays extensive details about the logging of all events and actions performed by users who are tasked with managing certificates. The following certificate events and actions are logged:

- Triggering of certificate discovery through any of the modes
- Pushing certificates into the server with either a managed or monitored status
- Creating, modifying, or deleting a certificate group
- Creating, modifying, or deleting a policy
- Modifying CA settings
- Triggering of the automatic certificate sync process
- Assigning or unassigning of a certificate group
- Deleting a certificate from the Server tab in the Inventory module
- Changing the status of action from the Server tab in the Inventory module
- Creating, modifying or deleting a Certificate Authority connector
  - Submitting, approving, rejecting, or implementing a new certificate request
  - Submitting, approving, rejecting, or implementing a renewal certificate request
  - Submitting, approving, rejecting, or implementing a revocation certificate request
- Creating, modifying or deleting an application connector
  - Submitting, approving, rejecting, or implementing a Certificate Push request
  - Submitting, approving, rejecting, or implementing a Rollback request
  - Disassociating a device from the connector
- Creating, modifying or deleting a monitor connector

## Configure Certificate Report Settings

Within the Dashboard module, it is possible to configure the following Server, Client, and Codesigning Certificate reports:

- Validation Status
- Certificate Summary Report
- Count by Issuer

Although the specific configuration fields vary depending on the report, the general configuration process is the same for all.

To configure the report settings:

1. Click and select **Dashboard**.
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 **Server Certificate**, **Client Certificate**, or **Code Signing Certificate** based on the report details that you want to export.
5. Locate the report widget that you want to configure, then click in the widget Command bar.
   The corresponding widget **Settings** screen opens.
6. Fill the mandatory fields.
7. When you have finished configuring the report details, click **Save**.

## Edit an Inframap or Blueprint Description

To edit the description of an Inframap or Blueprint:

1. Click and select **AppVision** > **Application**.
   The **Application** screen opens with the **Inframap** tab selected by default.
2. If you want to edit a Blueprint, click the **Blueprint** tab.
3. Click on the Inframap or Blueprint that you want to modify.
4. On the **Edit Description** screen that opens, modify the description that appears on the **Description** field.
5. Click **Save** to save your changes.

## Export a Certificate Report

You can export the following server and client certificate reports from the Dashboard:

- Validation Status
- Policy Compliance Report

To export details of one of the three reports listed above:

1. Click and select **Dashboard**.
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 **Server Certificate** or **Client Certificate** based on the report details that you want to export.
5. Locate the report widget that you want to export, then click in the widget Command bar.
6. On the **Export** screen that pops up, select one of the following file formats for the exported report:
   - **CSV**
   - **PDF**
7. Click **Export**.

## Firewall

Widgets within the Firewall Dashboard provides reports to monitor the Firewall rules and their performance.

To view firewall reports:

1. Click and select **Dashboard**.
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 **Firewall**.
5. Although each report displays the data differently, the same set of data is used to generate each report. When you click on any bar in a chart, an Inventory screen appears, displaying the firewall details corresponding to the bar you clicked.
6. The following reports are segregated and displayed as widgets on the Firewall screen:
   - **Unused Objects Report** - A doughnut chart that categorizes the list of unused objects fetched from the device based on its hit count. Selecting the **from** and **to** date and the **policy** name from the respective fields will retrieve the list of unused objects from the selected policy during the specified interval. For more details refer to the **View Hit Count for a Firewall Device** section of the guide.
   - **Optimization report for NAT** - A bar chart that shows the number of policies available for a defined NAT rule category. Select the policy from the **Policy Name** dropdown list for which you want to retrieve the report. When you can click on any bar, the control center view of the rule is displayed in the control grid (varies based on the policy, object, and rule parameters).

- Top 30 Most Used Security Rules - A bar chart that shows the most common security rules along with the number of times each has been used. Users can click the dropdown list at the top of the chart to select the policy whose security rules they want to view. Since all the entries do not fit on one screen, forward and back buttons beside the dropdown list allow users to advance to the other screens in the report.
- Top 30 Least Used Security Rules - A bar chart that shows the least common security rules along with the number of times each has been used. Users can click the dropdown list at the top of the chart to select the policy whose security rules they want to view. Since all the entries do not fit on one screen, forward and back buttons beside the dropdown list allow users to advance to the other screens in the report.
- **Optimization report for Security rules** - A bar chart that shows the number of policies available for a defined security rule category. Select the policy from the **Policy Name** dropdown list for which you want to retrieve the report. When you can click on any bar, the control center view of the rule is displayed in the control grid (varies based on the policy, object, and rule parameters).
- **Risk Report** - A bar chart that shows the number of devices, policy, application, or context (Cisco) that are in risk based on the set of violations and profiles association that is configured.

## WAF

The widgets within the WAF Dashboard provides reports for monitoring the Firewall rules and their performance.

To view the WAF reports:

1. Click  and select **Dashboard**.
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 **WAF**.
5. Although each report displays the data differently, the same set of data is used to generate each report. When you click on any bar in a chart, an Inventory screen appears, displaying the WAF details corresponding to the bar you clicked.
6. The following reports are segregated and displayed as widgets on the WAF screen:
   - **Risk Report** - A bar chart that shows the count of policies at risk based on the set of violations and profiles association configured for a device or an application. Select the device or application for which you want to retrieve the report. When you can click on any bar, the control center view of the rule is displayed in the control grid.

- **Risk Score Report** - A bar chart that shows the number of policies with the risk score based on the violation and profiles association that are configured for a device or an application. Select the device or application for which you want to retrieve the report. When you can click on any bar, the control center view of the rule is displayed in the control grid.
- **Learning Suggestion Report** - A bar chart that shows the number of learning suggestions learned for each policy from the F5 WAF device. Select the device for which you want to retrieve the report. When you can click on any bar, the learning suggestions view of the policy is displayed in the control grid.

## Connected Platform

The widgets displayed within the Connected platform dashboard are used for monitoring the usage of the AppViewX metric.

To view a widget related to the connected platform:

1. Click  and select **Dashboard**.
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 **Connected Platform**.
5. The following reports are segregated and displayed as widgets on the Connected platform screen:
   - **User information** - This is a metrics chart that has the details as individual metrics: Available role, Available Users, Available Usergroups, Total logins in AppViewX, and Unique logins in AppViewX. The top 20 roles and user details are shown in the popup as a pie chart for available roles and users.
   - **Inventory management** - This is a metrics chart that has the details as individual metrics: Available ADC Devices, Available SLB and GSLB Objects, Backup Generations, Available Firewall Devices, Available Firewall Rules, Available WAF Devices, and Available WAF Policies. The vendors and version details of the available ADC devices are shown as a bar chart.
   - **ADC Self Servicing - Dashboard** - This is a metrics chart that has the details as individual metrics: Available Dashboard, Available Widget, Enable Operations and Disable Operations. The count of ADC widget types is shown for the available widget types as a bar chart.
   - **ADC Self Servicing - Control Center** - This is a metrics chart that has the details as individual metrics: Topology View Creations, Enable Operations, Disable Operations, Set Ratio Operations, and View Graphics Operations. The count of control center operations is shown for the widget types as a bar chart.
   - **Certificate Management** - This is a metrics chart that has the details as individual metrics: Discovered Certificates, Available Certificates, Certificate Creations Regenerations, Certificate

Renewals, Certificate Revocations, Push Bind Operations, Push Only Operations, and Certificate Rollback Operations. The CA details of the available certificates are shown in the bar chart and certificate type details of the available certificates in the pie chart.

- **Change Control** - This is a metrics chart that has the details as individual metrics: Available Templates, Request Creations, Available Requests, Available Workflows, Workflow Request Creations, and Available Workflow Requests. The count of Studio operations is displayed.

**Note:** The export of the metrics option is supported by the connected platform.

## SSH Reports

The widgets displayed within the SSH dashboard provides reports to monitor the SSH keys managed at AppViewX.

To view SSH reports:

1. Click  and select **Dashboard**.
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 **SSH**.
5. Although each report displays the data differently, the same set of data is used to generate each report. When you click on any bar in a chart, an Inventory screen appears, displaying the certificate details corresponding to the bar you clicked.
6. The following reports are segregated and displayed as widgets on the SSH screen:
   - **Key Rotation Report by Month** - A bar chart that shows the total number of key rotations per month.
   - **Key Expiry Report** - A doughnut chart that categorizes the total number of SSH keys available in the system, with each sector representing a key expiry time. The colored bars represent the following statuses:
     - Green - Valid keys
     - Yellow - Keys with an expiry in 30 days
     - Powder Blue - Orphaned keys
     - Grey - New keys
     - Red - Expired keys
     - Orange - Keys with an expire in 10 days
     - Blue - Lifetime valid keys

- **Key Summary Report** - A bar chart that shows the count of SSH keys available for each key group such as All, Default_Host_Group, and Default_Key_Group. The colored bars represent the following key details:
  - Red - Standalone keys
  - Blue - Keys Mapped to Single User
  - Green - Keys Mapped to Multiple Users
- **Key Compliance Report** - A doughnut chart that shows the total number of SSH keys available in the system, with each sector representing the number of compliant and non-compliant keys.