Firewall User Guide

Version: 2023.1.0 FP3

Copyright AppViewX, Inc.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

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).

All other trademarks mentioned in this document are the property of their respective owners.

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
1.1	Updated the document for Release 2023.1.0 FP3.	June 2024
1.1	Updated the document for Release 2023.1.0 FP2.	February 2024
1.0	Initial release of document for Release 2023.1.0 FP1.	November 2023

About the Documentation

This guide explains the procedures for setting up and managing FIREWALL+ user functionality.

Documentation Conventions

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

Notice Icons

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

Audience

This document is intended for,

- Application teams
- Network Operations (NetOps)
- NetDevOps

- Traffic Management
- Automation and DevOps

Chapter 1: Getting Started

Overview

A multi-vendor firewall management solution is a comprehensive system that serves as a centralized platform for effectively controlling and monitoring the security policies of firewalls from various manufacturers within your network. This platform offers several advantages and capabilities:

- **Unified Control and Monitoring**: Instead of dealing with separate management interfaces for each firewall brand in your network, a multi-vendor solution brings them all under one roof. This unified control and monitoring make it easier for administrators to oversee and maintain security policies, irrespective of the firewall's make or model.
- **Simplified Rule Management**: Managing firewall rules can be complex, especially when dealing with multiple vendors. A multi-vendor solution simplifies this process by providing a common interface and rule structure. This streamlines rule creation, modification, and monitoring, reducing the chances of errors and misconfigurations.
- **Improved Automation**: Automation is a key component of modern network security management. A multi-vendor firewall management solution often includes automation features that help streamline tasks like rule creation, updates, and compliance checks. This not only saves time but also enhances the consistency and accuracy of firewall policies.
- **Risk and Compliance**: Maintaining a secure network is essential, and it involves identifying and mitigating security risks and ensuring compliance with industry regulations and organizational policies. The multi-vendor solution helps in risk assessment and compliance management by providing tools to monitor and enforce security policies consistently across different firewall brands.
- **Accommodating Diverse Firewall Brands**: In a typical organization, various firewall brands might be in use due to legacy systems, mergers, or specific security requirements. The multi-vendor solution is designed to accommodate this diversity, ensuring that the management platform can work with a wide range of firewall brands without compatibility issues.

Supported Web Browsers

Browser	Version	Notes
Firefox	Till latest (Version 84.0.4147.135)	
Chrome	Till latest (Version 80.0)	
IE	Limited support in 9, Full support from 10+	No support for IE9 post AppViewX Version 11.0

Browser	Version	Notes
Safari	Till latest (Windows - Version 5.1.7, macOS - Version 13.1.2)	From AppViewX Version 11.1
Opera	Till latest (Version 70)	From AppViewX Version 11.1

Related information
Vendor Specific Discover/Onboard Firewall Device

Chapter 2: Dashboard

About Dashboard

The dashboard allows you to manage, monitor, and interpret all the configured devices. It provides customizable widgets to get an overview of all the firewall devices, manager, and device under managers, firewall rules, firewall vendors, and configuration within the AppViewX platform. Customize your application dashboard with predefined and custom widgets as per the business requirements. You can create, save, download, e-mail, and align the dashboards.

The dashboard comes with a variety of pre-made dashboard widgets (components) that you can use to build a specific dashboard view that meets the different needs of your business. There are two types of dashboard,

- Insights - Firewall Summary (Default)
- Firewall.

Insights - Firewall Summary Dashboard

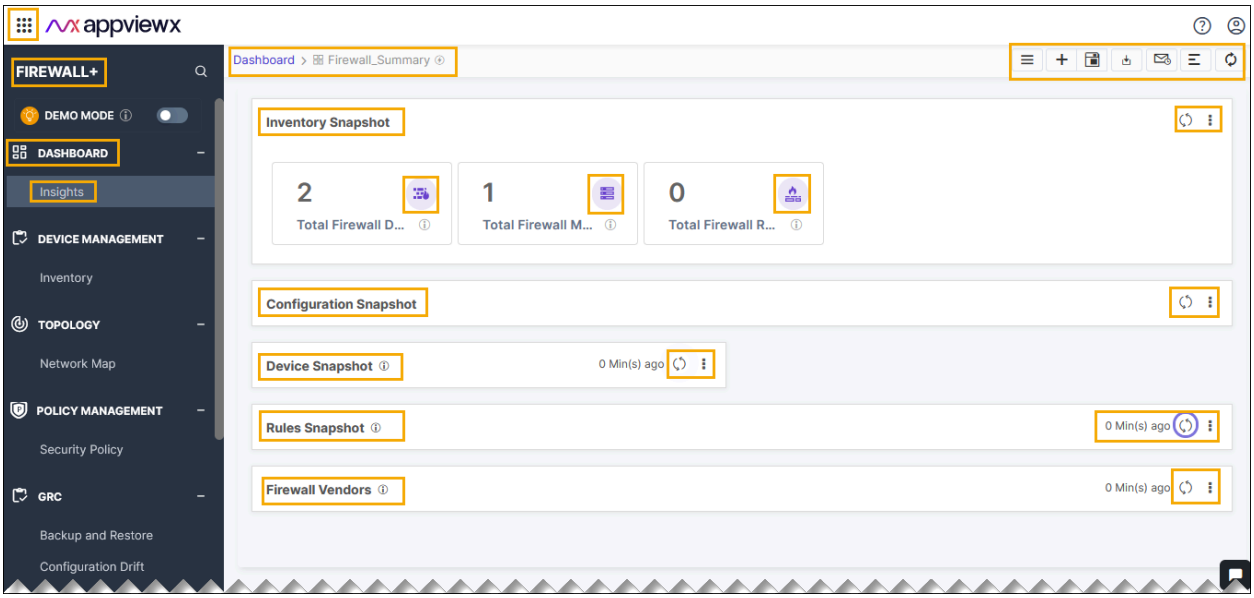
The INSIGHTS menu provides comprehensive information and analysis regarding the overall device/ object/application summary, compliance, and security of applications/devices delivered through the AppViewX infrastructure. The INSIGHTS menu populates with relevant data, once the devices have been successfully on-boarded and the applications are discovered.

The firewall summary dashboard manages and presents information about the firewall inventory, firewall rules, firewall vendors, and configurations within the AppViewX platform.

To access the INSIGHTS page,

- Go to **Menu** > **FIREWALL+** > **INSIGHTS**.

  The **Firewall_Summary** page is displayed.



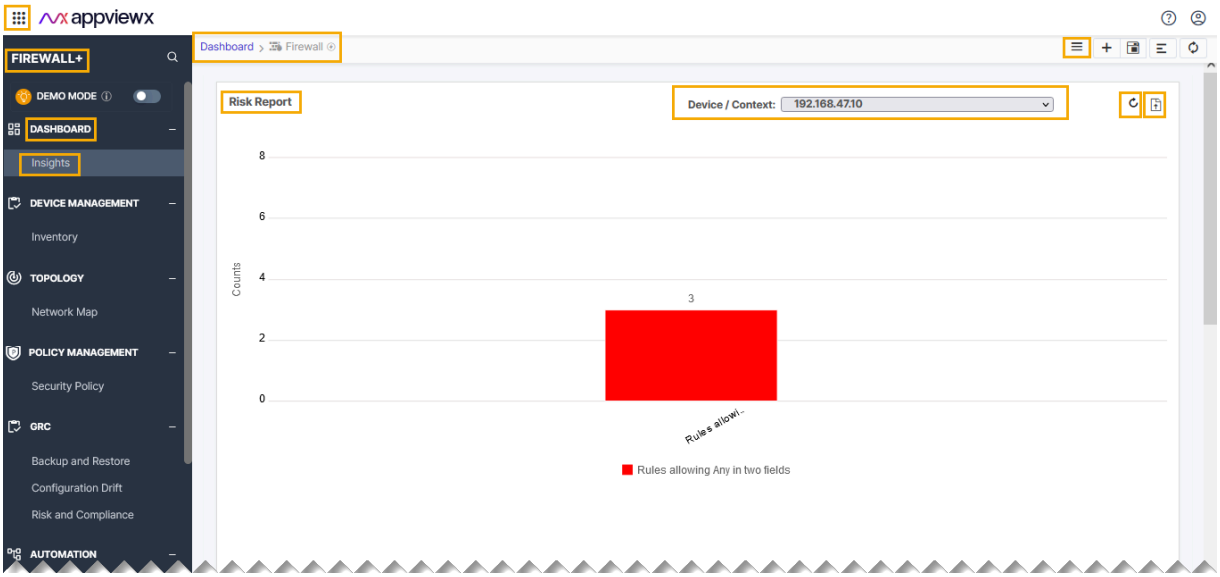
Firewall Dashboard

The firewall dashboard manages and displays the Optimization report supported by product for security rules and NAT rules, Firewall rule compliance report, and Risk report of the AppViewX platform.

To access the Firewall page,

1. Go to **Menu** > **FIREWALL+** > **INSIGHTS**
2. Click the  (**Dashboard Inventory**) icon, and then select Firewall from the list.

   The **Firewall** dashboard page is displayed.



Firewall Summary Snapshots

The firewall summary snapshot provides a visual representation of the Inventory, Configuration, Rules, and Firewall in the form of a graphical display. Click on the corresponding snapshot and a window will appear with the relevant details. The snapshot visual representation includes areas that display breakdown of details based on different categories or criteria.

The snapshots allows you to,

-  collapse the dashboard widget.
-  expand the dashboard widget.
-  minimize the dashboard widget
-  maximize the dashboard widget.
-  download the dashboard details in the <.pdf> format.
-  export the dashboard details in the excel format.

The following snapshots are available in the firewall summary dashboard.

- Inventory Snapshot
  - Total Firewall Devices – It presents the information about the inventory firewall, inventory managers, and target devices in managers.
  - Total Firewall Manager - It presents the information about the firewall managers in inventory (vendor and platform).
  - Device under managers - It presents the information about the target devices in the managers.
  - Total firewall rules - It presents the information about the devices and managed in inventory.
- Configuration snapshot - It presents the number of backups for the configuration.
- Device snapshot - It presents the number of managers and firewall.
- Rules snapshot - It presents the number of Security rules, NAT rules and Route rules.
- Firewall vendors - It presents the information counts based on each vendor in the device.

Collapsing the Snapshots

To collapse the snapshots,

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. On the desired snapshots, click the (**three dotted**) icon.
3. Select the (**Collapse**) icon.

   The snapshot/widget is collapsed.

Expanding the Snapshots

To expand the snapshots,

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. On the desired snapshots, click the (**three dotted**) icon.
3. Select the (**Expand**) icon.

   The snapshot/widget is collapsed.

Minimizing the Snapshots

To minimize the snapshots,

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. On the desired snapshots, click the (**three dotted**) icon.
3. Select the (**Minimize**) icon.

   The snapshot/widget is collapsed.

Maximizing the Snapshots

To maximize the snapshots,

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. On the desired snapshots, click the (**three dotted**) icon.

3. Select the (**Maximize**) icon.

   The snapshot/widget is collapsed.

Downloading/Exporting the Snapshots

You can download/export the snapshots and widgets within the snapshots in the firewall summary dashboard.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. On the desired snapshots, click the (**three dotted**) icon.

3. Select the download/export option.
   - Download as PDF
   - Export as Excel
   - Export as CSV.

   The file will be downloaded/exported and saved in your desktop's Downloads folder.

- Widgets

Widgets

You can download/export the widgets from the inventory widgets from the firewall summary dashboard.

Downloading the Inventory Widgets for Total Firewall Devices

To download the total firewall device, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. • On the **Inventory Snapshot** > **Total Firewall Devices** widget, click the (**ge-firewall**) icon.

   The **Total Firewall Devices** pop-up window is displayed.

3. Click **Select download** drop-down menu, and then select the type of format that you want to download. Available type of formats are,
   • Download as PDF
   • Download as Excel
   • Download as CSV.
4. The file will be downloaded and saved in your desktop's Downloads folder.

Downloading the Inventory Widgets for Total Firewall Managers

To download the total firewall device, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. • On the **Inventory Snapshot** > **Total Firewall Managers** widget, click the  (**device2**) icon.

   The **Total Firewall Managers** pop-up window is displayed.

3. Click the **Vendor** or **Platform** tab that you want to download/export
4. Click **Select download** drop-down menu, and then select the type of format that you want to download. Available type of formats are,
   • Download as PDF
   • Download as Excel
   • Download as CSV.
5. The file will be downloaded and saved in your desktop's Downloads folder.

Downloading the Inventory Widgets for Devices Under Managers

To download the total firewall device, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. • On the **Inventory Snapshot** > **Devices Under Managers** widget, click the  (**ge-firewall**) icon.

   The **Devices Under Managers** pop-up window is displayed.

3. You can select list in the below order from the drop-down list.

- Device Serial Number
- IP
- Host Name
- Device Version.

4. Click **Select download** drop-down menu, and then select the type of format that you want to download. Available type of formats are,
   - Download as PDF
   - Download as Excel
   - Download as CSV.
5. The file will be downloaded and saved in your desktop's Downloads folder.

Downloading the Inventory Widgets for Total Firewall Rules

To download the total firewall device, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. • On the **Inventory Snapshot** > **Total Firewall Rules**, click the  (**firewall**) icon.

   The **Total Firewall Rules** pop-up window is displayed.

3. Click **Select download** drop-down menu, and then select the type of format that you want to download. Available type of formats are,
   - Download as PDF
   - Download as Excel
   - Download as CSV.
4. The file will be downloaded and saved in your desktop's Downloads folder.

Creating Firewall Summary Dashboard

The dashboard allows you to manage, monitor, and interpret all the configured applications and their objects. It provides customizable widgets to get an overview of all the AppViewX Applications. Customize your Application dashboard with predefined and custom widgets as per the business need.

Creating Firewall Summary Dashboard

To create dashboard, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click  (**Create**) icon on the top-right of the page.

   The **Create dashboard / widget** pop-up window is displayed.

3. On the **Create dashboard / widget** pop-up window, enter a name for the new dashboard.

4. Select a solution from the Select Solution drop-down list to which you want the widget to be created: ADC, Firewall, Certificate, WAF.

5. Select the solution from the drop-down list that you want the corresponding widgets to be managed.

6. Select the **Widget Type** as **Custom** or **Default**.
7. If the Custom radio button is selected in Step 5, then choose any one of the below options from the Select Widget dropdown.
   - Custom reports
   - reportEngine
   - reportEngineCanvas.
8. If the default radio button is selected in Step 5, choose the default widgets you want to manage/ monitor in the custom dashboard. Select the default widgets you want to manage/monitor in the custom dashboard.

9. Click **Create**.

   You are redirected to the widget configuration screen, which varies according to the widget selected.

Dashboard Functionalities

Saving Dashboard

The dashboard allows you to save the changes when you drag and drop the widgets to organize them in the dashboard, complete the following steps to save the changes.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. After making necessary changes in the dashboard, click the  (**Save dashboard**) button in the Command bar.

   A pop-up message appears at the top of the dashboard, "Dashboard saved successfully."

Downloading Dashboard

To download a dashboard,

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click the  (**Download as PDF**) button in the Command bar at the top of the screen. The Import screen appears.

   A pop-up message appears at the top of the dashboard, "Dashboard saved successfully."

Schedule and Email Reports

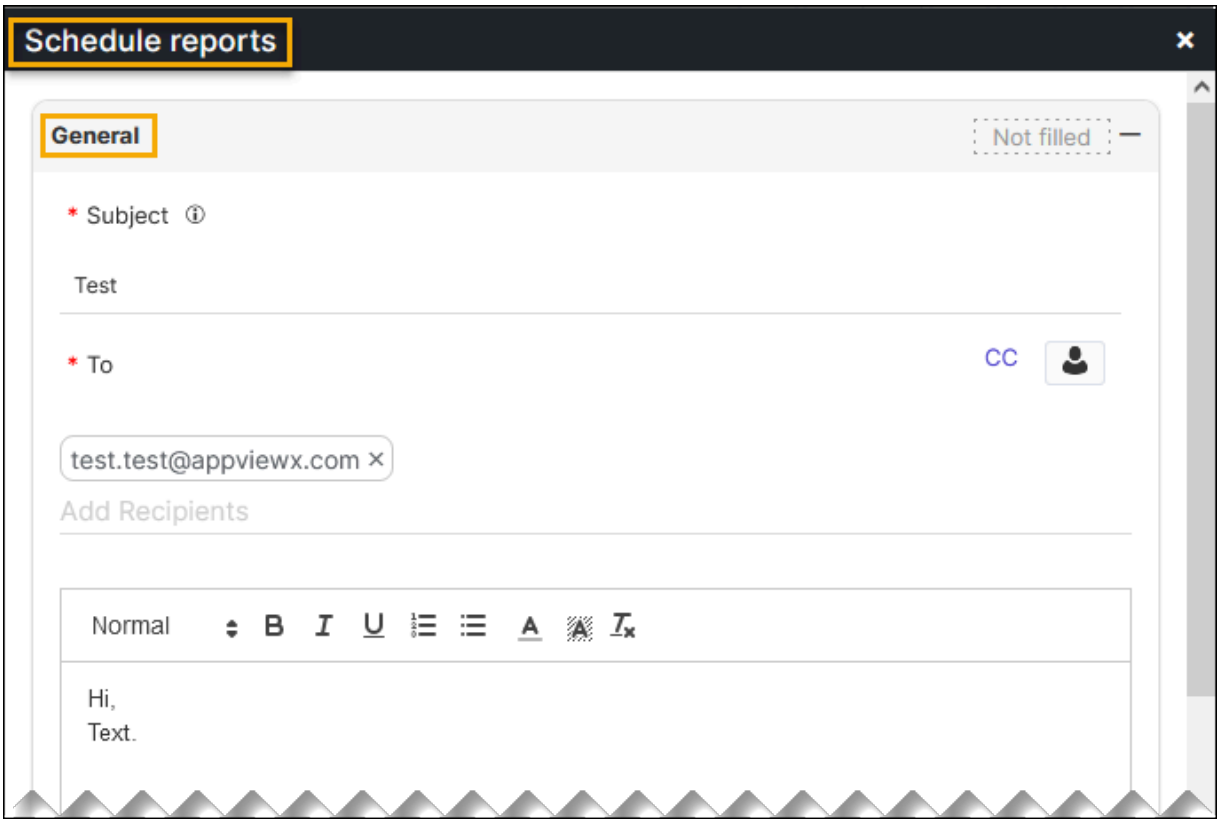
Based on your permissions, you can schedule and share a dashboard via e-mail. To share scheduled dashboard via email, do the following steps:

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

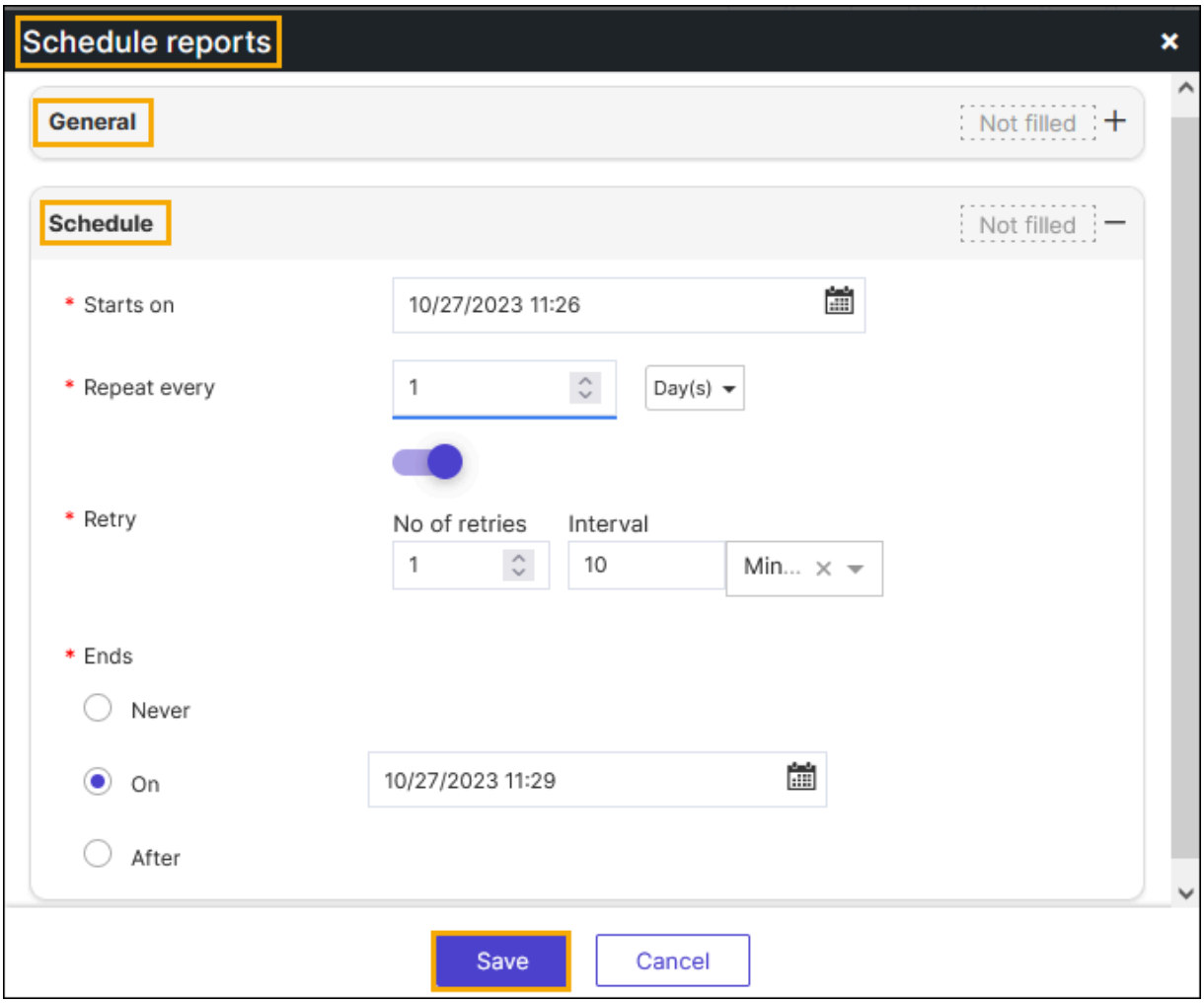
   The firewall summary dashboard is displayed.

2. Click the  (**Schedule and Email Reports**) icon.

   The Schedule Reports window is displayed.


Schedule reports
General
Not filled
* Subject
Test
* To
CC
test.test@appviewx.com ×
Add Recipients
Normal
Hi,
Text.

3. Enter the required details in the **General** and **Schedule** section in the **Schedule reports** page.



Aligning Dashboard

Based on your permissions, you can align a dashboard. To align the dashboard, do the following steps:

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click the (**Align**) button.
3. Make sure that the dashboard widgets are aligned in the right.

Refreshing Dashboard

Based on your permissions, you can align a dashboard. To align the dashboard, do the following steps:

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click the  (**Refresh**) button.

3. Make sure that the dashboard widgets are refreshed.

> **Note:** You can also refresh individual widgets, using the refresh button.

Firewall Dashboard

The firewall dashboard manages and displays the Optimization report supported by product for security rules and NAT rules, Firewall rule compliance report, and Risk report of the AppViewX platform.

Creating the Firewall Dashboard

To create dashboard, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click  (**Dashboard inventory**) icon on the top-right of the page.

   The Dashboard list page appears.

3. Select **Firewall** from the list of dashboards.

   The firewall dashboard is displayed.

4. Click  (**Create**) icon on the top-right of the page.

   The **Create dashboard / widget** pop-up window is displayed.

5. On the **Create Dashboard/Widget** pop-up window, enter a name for the new dashboard.
6. Select a solution from the **Select Solution** drop-down list to which you want the widget to be created:
   - ADC
   - Firewall
   - Certificate
   - WAF.
7. Select the **Widget Type** as **Custom** or **Default**.

8. If the Custom radio button is selected in Step 5, then choose any one of the below options from the **Select Widget** drop-down:
   • Custom reports
   • reportEngine
   • reportEngineCanvas.
9. If the default radio button is selected in Step 5, choose the default widgets you want to manage/ monitor in the custom dashboard from the **Choose widgets** list.
10. In the **Widget name** field, enter a name for the new widget.
11. Click **Create**.

    You are redirected to the widget configuration screen, which varies according to the widget selected.

Saving Dashboard

The dashboard allows you to save the changes when you drag and drop the widgets to organize them in the dashboard, complete the following steps to save the changes.

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click  (**Dashboard inventory**) icon on the top-right of the page.

   The Dashboard list page appears.

3. After making necessary changes in the dashboard, click the  (**Save dashboard**) button in the Command bar.

   A pop-up message appears at the top of the dashboard, "Dashboard saved successfully."

Aligning Dashboard

Based on your permissions, you can align a dashboard. To align the dashboard, do the following steps:

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click  (**Dashboard inventory**) icon on the top-right of the page.

   The Dashboard list page appears.

3. Click the  (**Align**) button.
4. Make sure that the dashboard widgets are aligned in the right.

Refreshing Dashboard

Based on your permissions, you can align a dashboard. To align the dashboard, do the following steps:

1. Go to **Menu** > **FIREWALL+** > **DASHBOARD** > **Insights**.

   The firewall summary dashboard is displayed.

2. Click  (**Dashboard inventory**) icon on the top-right of the page.

   The Dashboard list page appears.

3. Click the  (**Refresh**) button.

4. Make sure that the dashboard widgets are refreshed.

> **Note:** You can also refresh individual widgets, using the refresh button.

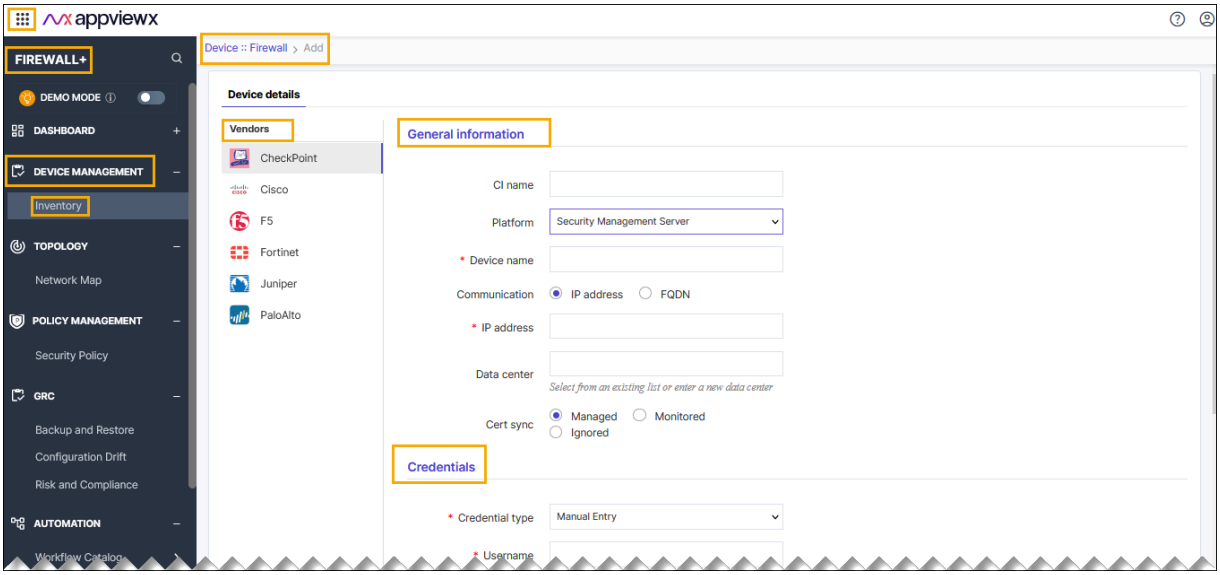
Chapter 3: Device Management

Discover/Onboard an Firewall Device

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

To onboard a device into Device Inventory,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click the + (**Add**) icon located upper right corner.
   The **Add** page appears.



3. Select the vendor from the left side bar.
4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.

Field	Description
Platform	Select the platform from the drop-down list. The available options are, • Security Management Server • MultiDomain Security.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device.  **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

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

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

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

- To discard the changes, click the Cancel button.

• Vendor Specific Discover/Onboard Firewall Device

Vendor Specific Discover/Onboard Firewall Device

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

• Prerequisites for Vendor Onboarding
• Adding a CheckPoint Firewall Device
• Adding a Cisco Firewall Device
• Adding a F5 Firewall Device
• Adding a Fortinet Firewall Device
• Adding a Juniper Firewall Device
• Adding a PaloAlto Firewall Device

Prerequisites for Vendor Onboarding

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
IP Address/ FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN	IP address / FQDN
User Privilege	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark	• Username / Password • Credential List AppViewx/ Cyberark
Enable Password	Required	Not Required	Not Required	Not Required	Required
License Check	Not Required	Not Required	Not Required	Not Required	Not Required
Services and Prot for AppViewX communication	Port number: 22 (SSH)	Port number: 22 (SSH)	Port number: 443 (API)	Port number: 443 (API)	Port number: 22 (SSH, till R77) and 443 (API, from R80)
Internet Access/ Proxy if required	Not Required	Not Required	Not Required	Not Required	Not Required
Location from which the certificates are discovered if Certificate Managed.	Certificates are fetched by issuing a direct command to the device through SSH.	Not supported	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct API call to the device.	Certificates are fetched by issuing a direct command to the device through SSH. Directory in the device are /web/ conf/server.crt /web/conf/ server.key

Supported Vendors	Cisco ASA	Juniper	PaloAlto	Panorama	Checkpoint CMA
Note	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.	For VW action items, you need credentials with write privilege.

Adding a CheckPoint Firewall Device

Prerequisites

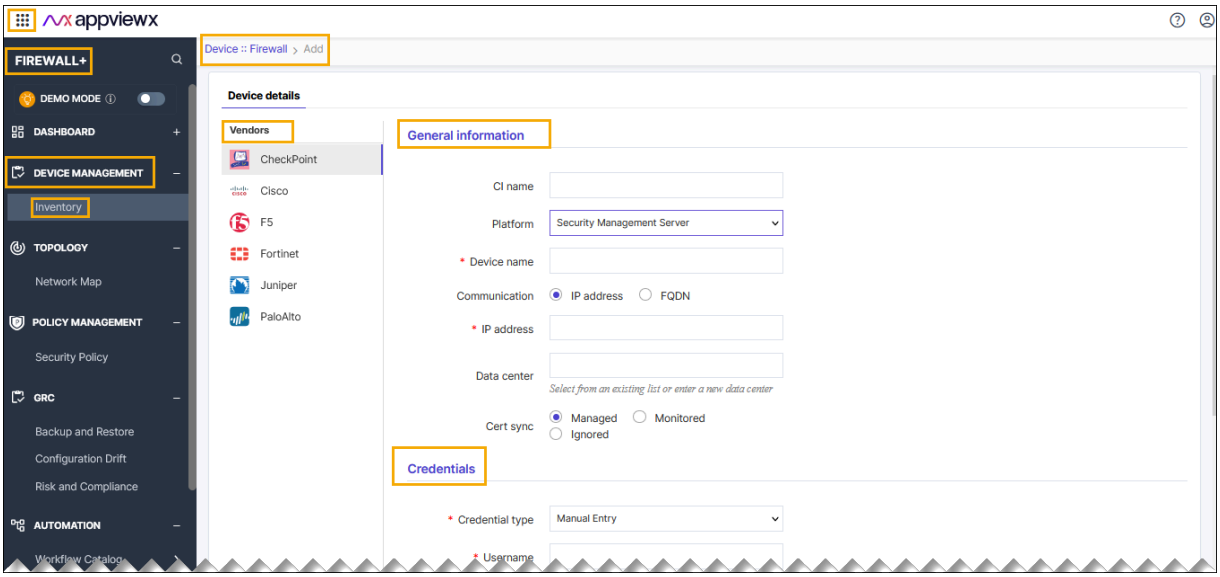
- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port numbers 22 (SSH, till R77) and 443 (API, from R80)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**:
  - Certificates are fetched by issuing a direct command to the device through SSH.
  - Location in the device:
    - /web/conf/server.crt
    - /web/conf/server.key

Note: For Visual Workflow action items, you will require credentials with write privilege.

Configuring a CheckPoint Firewall Device

To add a CheckPoint device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **CheckPoint** vendor from the left command bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • Security Management Server • MultiDomain Security.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

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

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

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

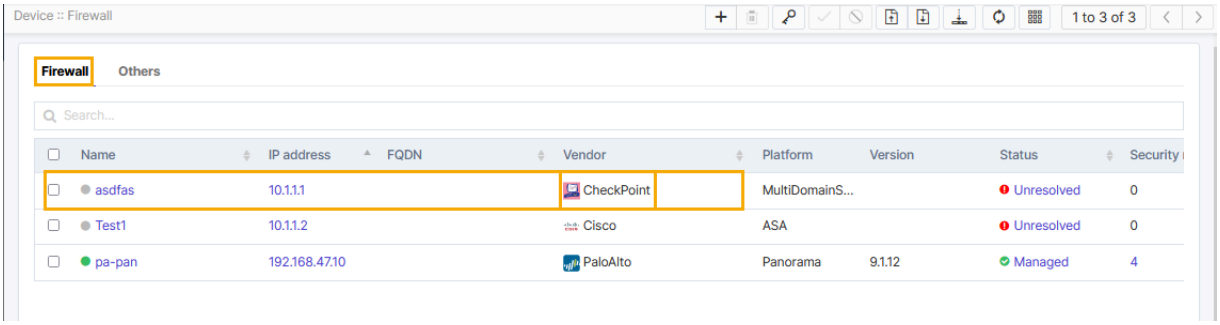
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the CheckPoint Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a Cisco Firewall Device

Prerequisites

- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.

- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port numbers 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Certificates are fetched by issuing a direct command to the device through SSH.

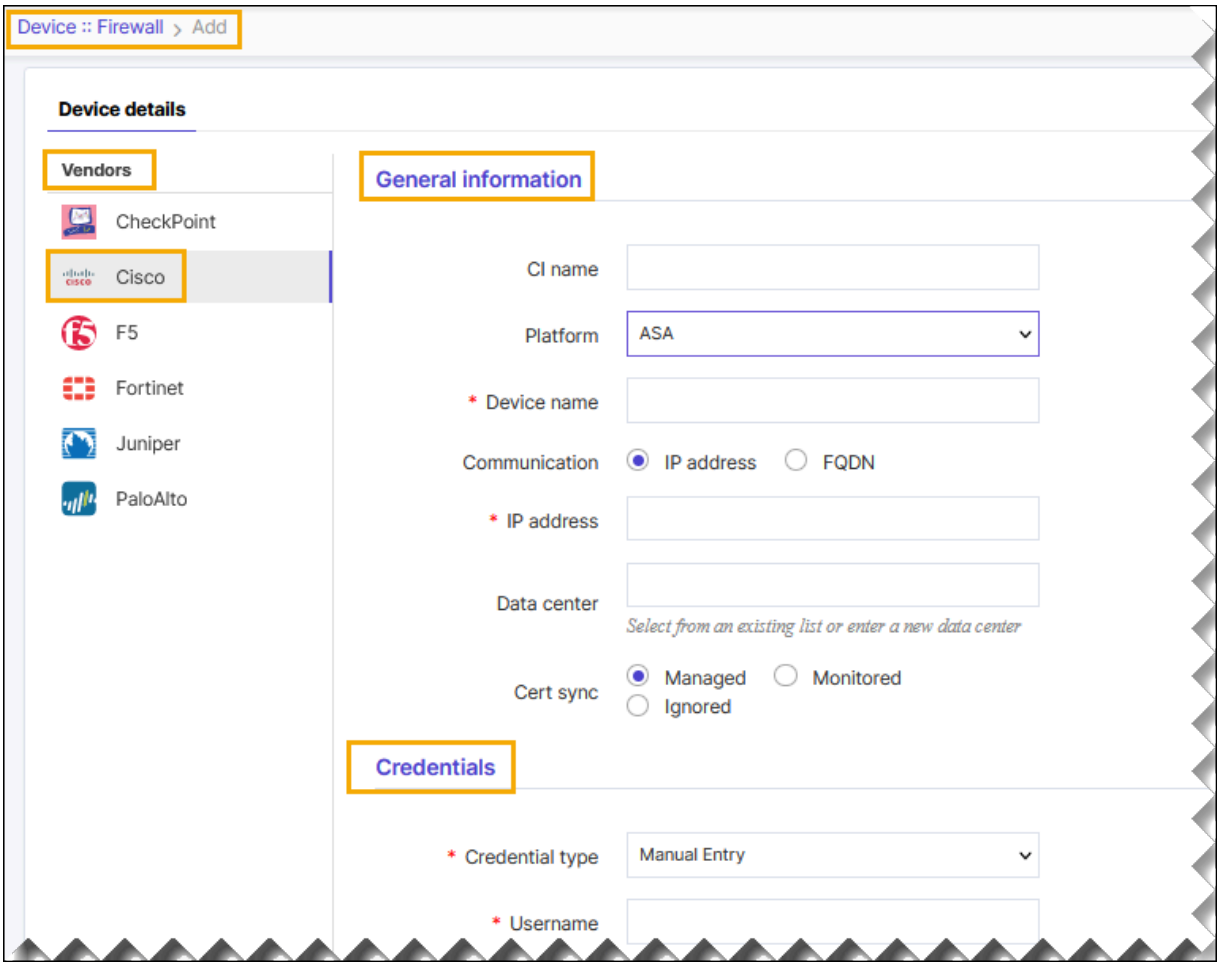
Note: For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Cisco Firewall Device

Prerequisites

To add a Cisco device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click  (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **Cisco** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • ASA.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

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

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

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

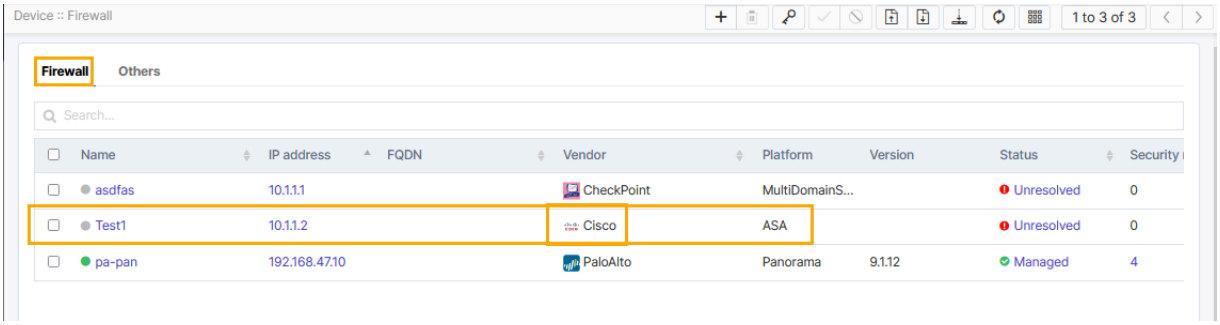
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the Cisco Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a F5 Firewall Device

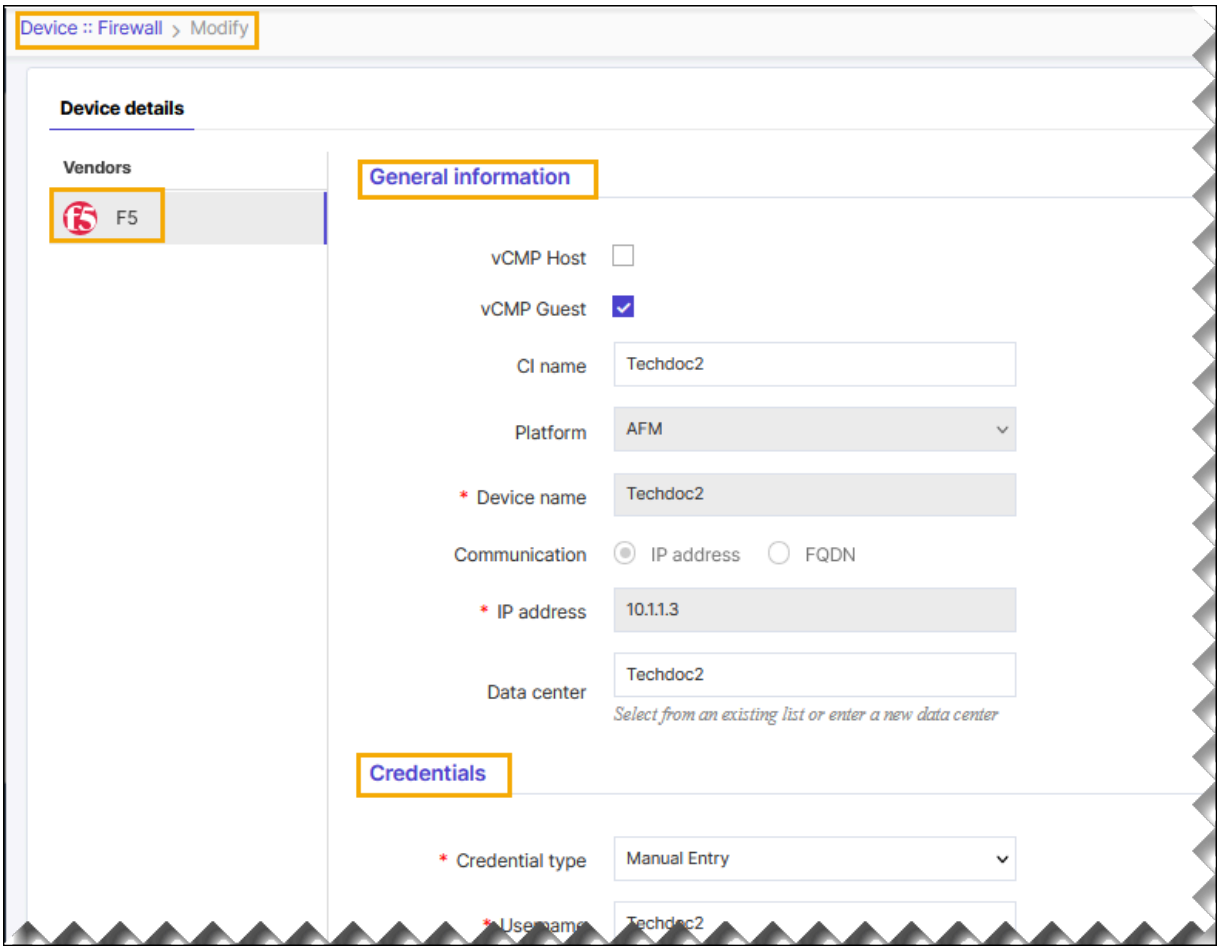
Configuring a F5 Firewall Device

To add a F5 device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.

The **Add** page appears.

3. Select the **F5** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
vCMP Host	Select the check box to add host based device if required.
vCMP Guest	Select the check box to add device as guest if required..
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • AFM.
***Device name**	Unique custom identifier of your device.

Field	Description
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device.  **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

6. **Note:** This step is applicable only if you have selected **vCMP Host** check box in the **General Information** section.

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

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

> **Note:**
> - By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
> - By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

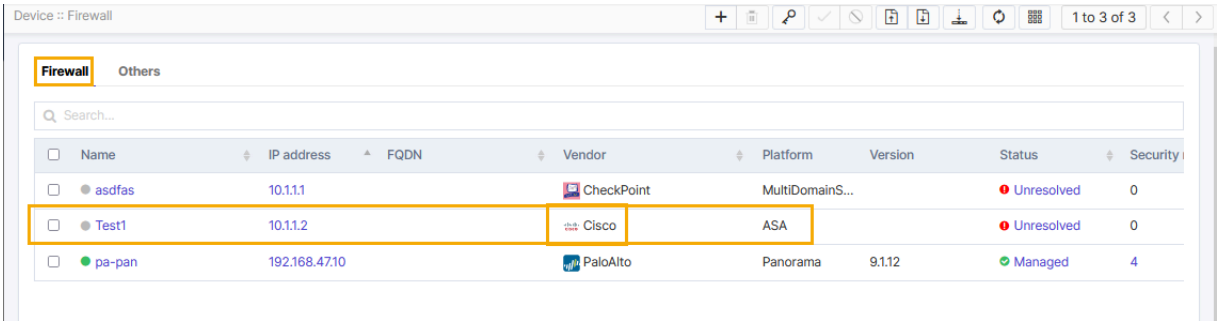
> **Note:**
> - To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the F5 Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a Fortinet Firewall Device

Prerequisites

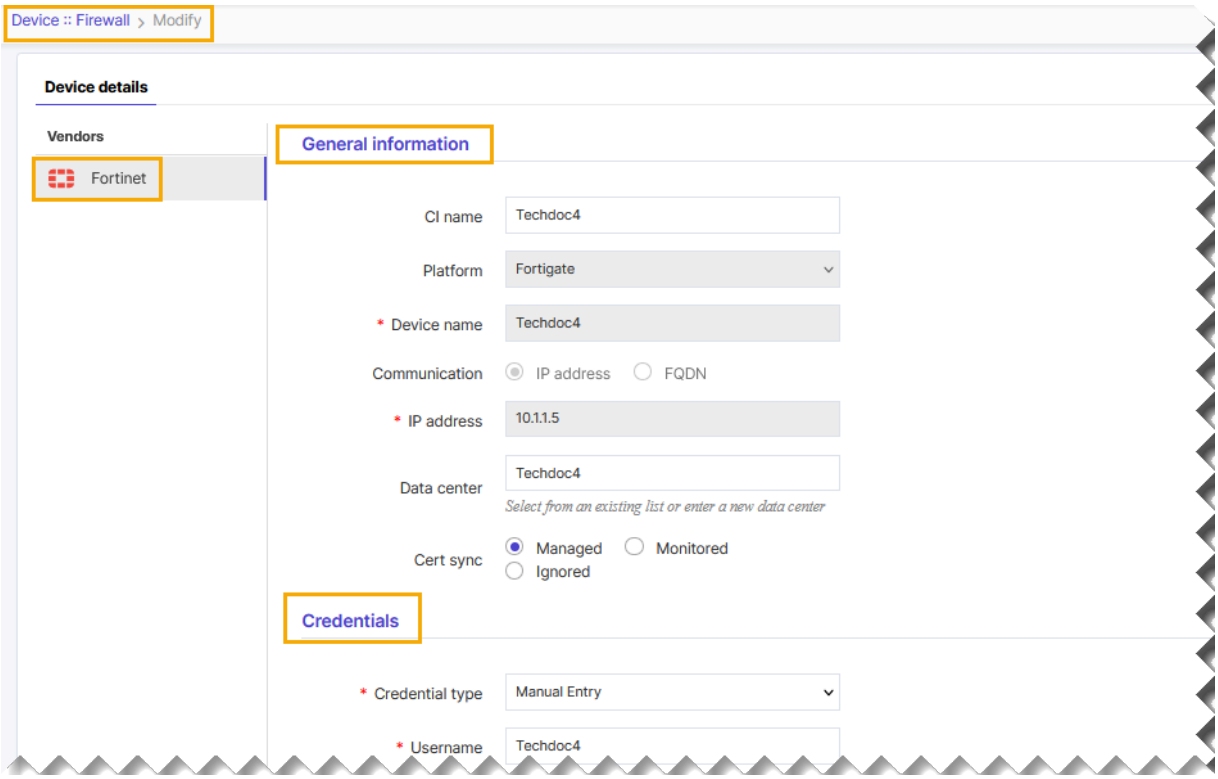
- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**: Username/Password
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)

> **Note:** For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Fortinet Firewall Device

To add a Fortinet device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **Fortinet** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • ASA.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

6. Enter or select the field information in the **Certificate specific details** section:

Field and Description Table

Field	Description
Discover Private Keys	Select the check box.
Private Key Default Password	Enter the default password.

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

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

Note:
- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

8. Click the **Save** button to add an Firewall device.

Note:
- To discard the changes, click the Cancel button.

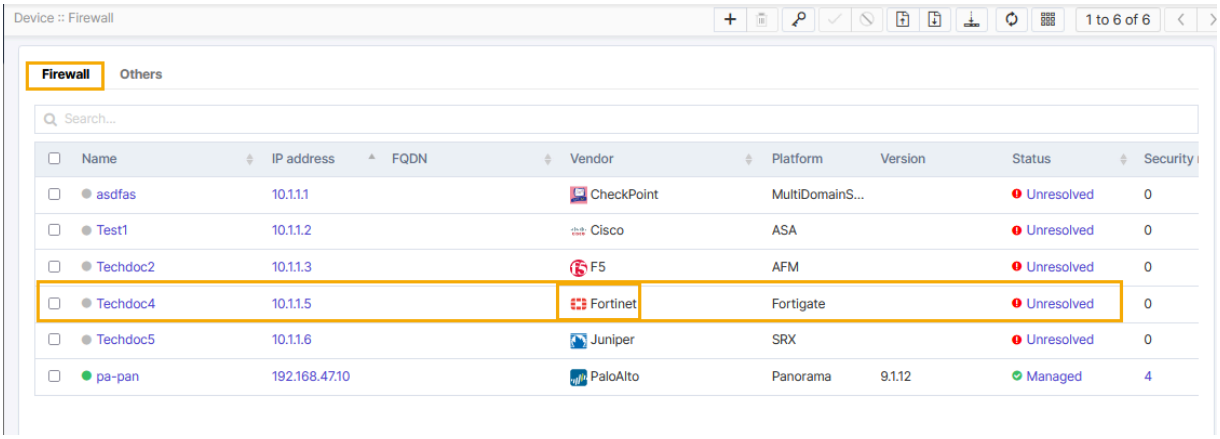
A pop-up message is displayed as **Device added successfully**.

Validating the Fortinet Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.

2. Search the device name and validate whether the device is added successfully.



Adding a Juniper Firewall Device

Prerequisites

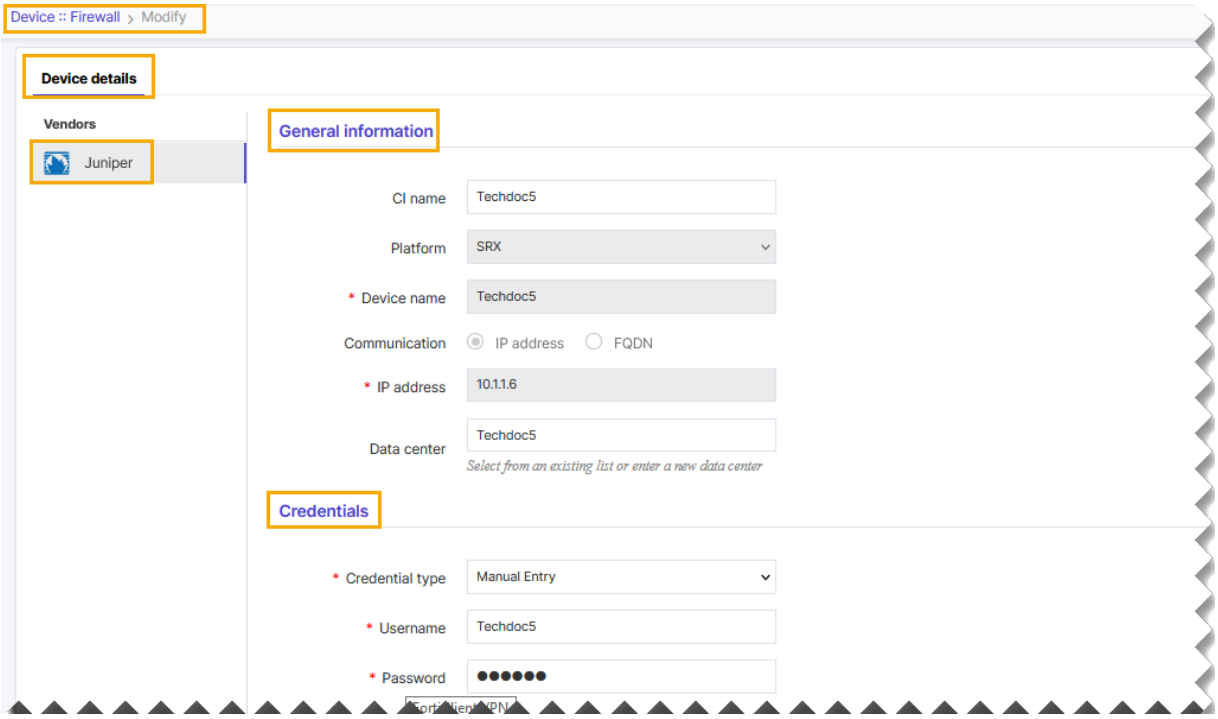
- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port number 22 (SSH)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Not supported

> **Note:** For Visual Workflow action items, you will require credentials with write privilege.

Configuring a Juniper Firewall Device

To add a Juniper device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **Juniper** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • SRX.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

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

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

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

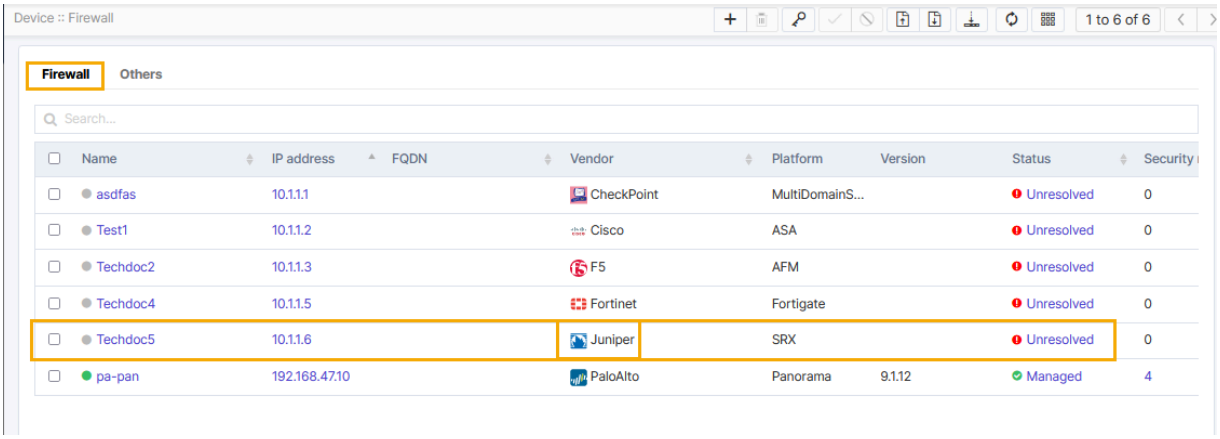
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the Juniper Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Adding a PaloAlto Firewall Device

Prerequisites

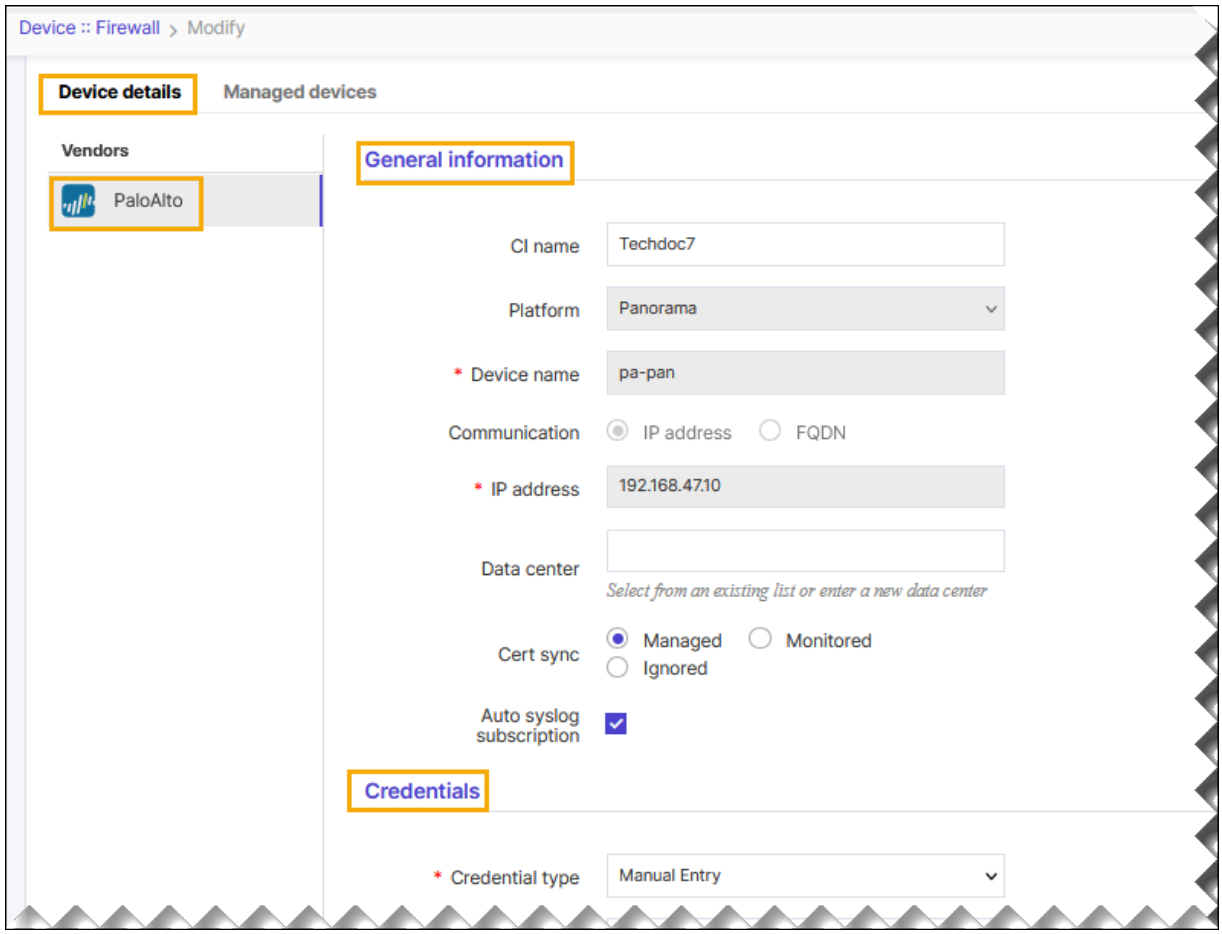
- **General prerequisites**:
  - Ensure communication between AppViewX and the firewall is enabled.
  - AppViewX needs an internet or proxy connection to communicate with the firewall via the REST API.
  - Valid firewall account details, including API tokens/keys and user credentials, are necessary.
  - The API must have elevated (admin) permissions to read and modify SSL certificates.
- **IP Address/FQDN**: IP address or FQDN
- **User Privilege**:
  - Username/Password
  - Credential List AppViewX/CyberArk
- **Enable Password**: Required
- **License Check**: Not required
- **Services and Port for AppViewX Communication**: Port number 443 (API)
- **Internet Access/Proxy**: Not required
- **Location from which the certificates are discovered if Certificate Managed**: Certificates are fetched by issuing a direct API call to the device.

> **Note:** For Visual Workflow action items, you will require credentials with write privilege.

Configuring a PaloAlto Firewall Device

To add a PaloAlto device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. In the **Firewall** tab, click + (**Add**) icon located upper right corner.
   The **Add** page appears.
3. Select the **PaloAlto** vendor from the left side bar. bar.



4. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
CI name	Name of the CI.
Platform	Select the platform from the drop-down list. The available option is, • Firewall • Panorama.
***Device name**	Unique custom identifier of your device.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
Communication	The communication mode that firewall devices can be added to AppViewX. The possible communication modes are: • **IP Address** - The IP Address can be IPV4 and it can be either management IP or Self IP of the Firewall device. By default, the IP address has been selected. • **FQDN** - On adding the device with FQDN, it will be resolved to an IP address and communication to the device will be made through it. If the FQDN is resolved to more than one device IP, AppViewX will choose a random IP for communication.
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
Cert sync	Provision to discover and manage the SSL certificates from the firewall devices. The possible Cert syncs are: • **Managed** - All SSL certificates will be discovered and added to AppViewX certificate inventory and used for certificate lifecycle management like renew, revoke, etc. • **Monitored** - All SSL certificates will be discovered and will not have any CA-related communication. • **Ignored** - No SSL certificates will be discovered from the firewall device. **Note:** The certification sync is based on the license applied.
**: Mandatory fields*	

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

Field and Description Table

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

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

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

Note:

- By clicking the Add button, multiple devices can be added as secondary devices and all the devices will be available in the grid.
- By managing the Primary and Secondary devices in AppViewX during the device flips, traffic routing and management can be seamlessly handled in AppViewX.

7. Click the **Save** button to add an Firewall device.

Note:

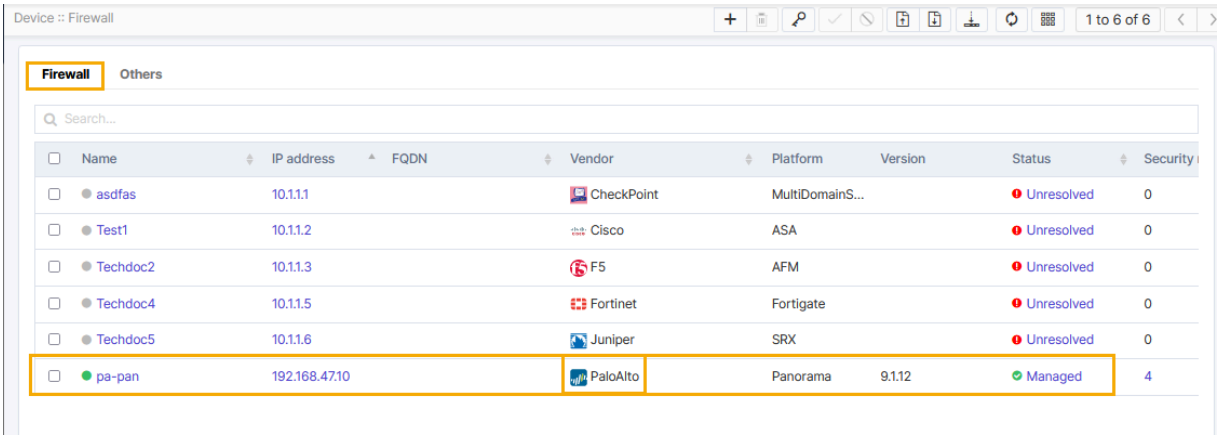
- To discard the changes, click the Cancel button.

A pop-up message is displayed as **Device added successfully**.

Validating the PaloAlto Device Addition

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Search the device name and validate whether the device is added successfully.



Deleting Firewall Device(s)

To delete Firewall device(s),

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Select the desired firewall device(s) to delete.

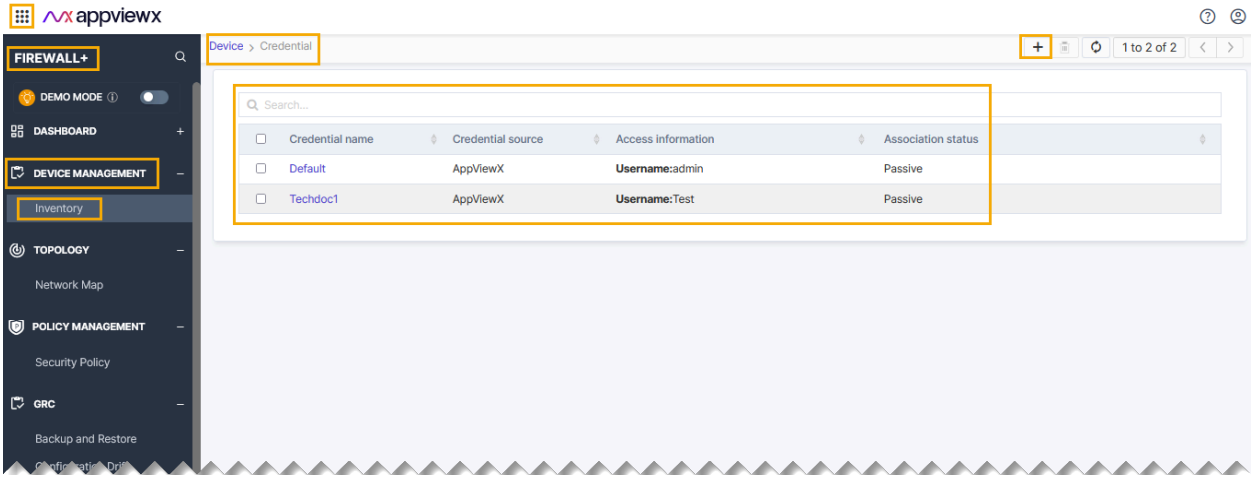
3. Click the  **Delete** button in the Command bar.
   The **Delete** confirmation pop-up window appears.
4. Click **Yes** to delete the selected Firewall device(s).

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

Related information
Vendor Specific Discover/Onboard Firewall Device

Managing Credential

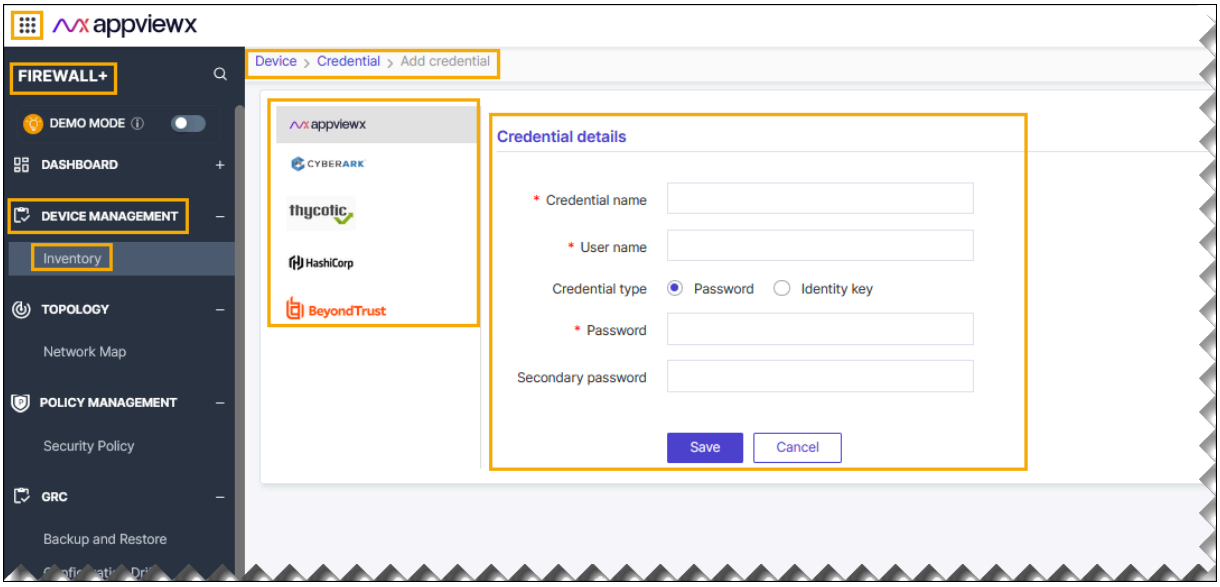
The firewall inventory management within the AppViewX application streamlines the process of managing and securing firewall credentials. It provides a secure and efficient way to store, control access to, and monitor the use of firewall credentials. It enhances the security and manageability of an organization's network infrastructure.



To add credential,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Click the  (**Credential**) icon from the right-top of the page.
   The credential home page is displayed.
3. Click the  (**Add credential**) icon from the right-top of the page.

The Add credential page is displayed.



4. Select the device from left bar.
5. Enter or select the field information in the **Credential details** section.

Field and Description Table

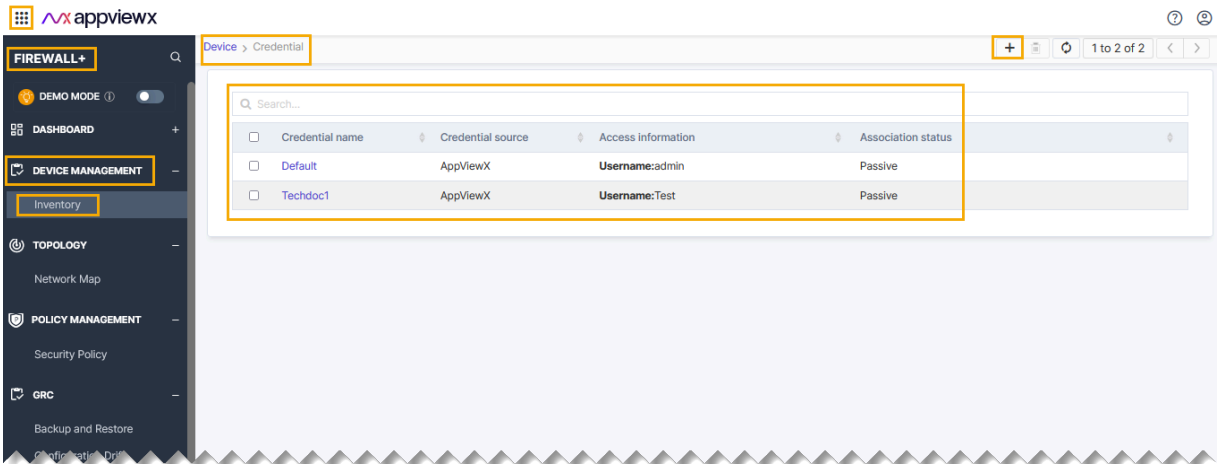
Field	Description
***Credential name**	Name of the credential.
***User name**	Enter name of the user.
Credential type	Click radio button to select the desired type of credential. Available types are, • Password • Identity key.
***Password**	If the credential type is selected as password, then enter the valid password in this field.
Identity key	If the credential type is selected as Identity key, then upload the private key that is used in SSH for granting access to device in the below foramt. • .prem • .txt • _rsa • _dsa • .ppk.

Field	Description
Passphrase	If the credential type is selected as identity key, then enter the passphrase in this field.
Password	If the credential type is selected as password, then enter the valid password in this field.
Secondary Password	If the credential type is selected as password, then enter the valid password in this field.
**: Mandatory fields*	

Validating the Credential Type

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

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Click the  (**Credential**) icon from the right-top of the page.
   The credential home page is displayed.



3. Search the device name and validate whether the device is added successfully.

Related information
Vendor Specific Discover/Onboard Firewall Device
Deleting Firewall Device(s)

Manage and Unmanage Devices

To manage or unmanage devices,

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

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

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

Related information
Vendor Specific Discover/Onboard Firewall Device
Deleting Firewall Device(s)
Managing Credential

Export Device Details

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

To export the details of one or more devices,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. If the device you want to export is not listed on the screen, run a search to locate it.
3. Click the checkbox beside the device name. If you are exporting details of multiple devices of the same kind, select the checkboxes for each one.
4. Click the **Export** icon in the Command bar at the upper right of the screen.
5. On the **Export** pop-up screen that appears, select the type of information you want to export:

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

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

Related information
Import Devices

Import Devices

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

To import devices using a .csv file,

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

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

Related information
Export Device Details

Manually Fetch the Configuration for a Device

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

To manually get the configuration for a device,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. If the device is not listed on the screen, run a search to locate it.

3. Click the checkbox beside the device name. If you want to fetch configurations for multiple devices of the same type, select their checkboxes, too.
4. Click the  **Fetch Config** icon in the Command bar.
5. A notification appears at the top of the screen stating, "**Fetch config has been triggered for the device(s).**".

Related information
Export Device Details
Import Devices

Customizing Columns

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

To customize columns,

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Click the  **Columns** icon in the Command bar.
   The **Columns** pop-up opens.
3. In the Columns pop-up, you can modify the columns by doing any of the following or in the combination:

   a. Select or deselect the desired columns to be displayed in the **Firewall** tab.

   b. Alter the order of the column by dragging the column name to the desired order.

   c. Select all the available columns by clicking the **Select all** checkbox.

   d. Reset to the previous column selection by clicking the "**Reset to previous column selection**".
4. Click the **Save** button.

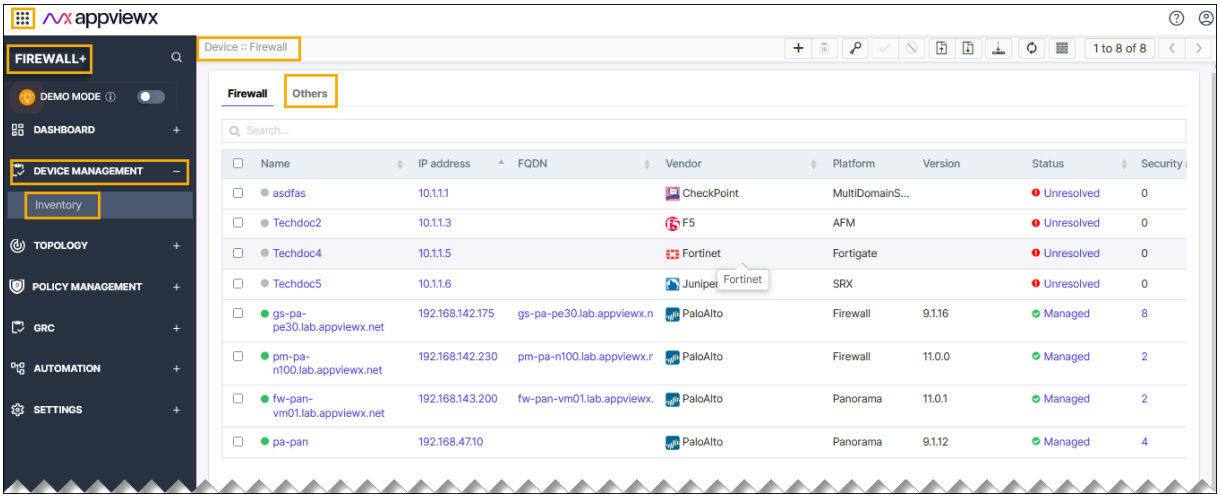
> **Note:** To discard the changes, click the **Cancel** button.

Related information
Export Device Details
Import Devices
Manually Fetch the Configuration for a Device

Device Management Others

The purpose of inventory management for other vendors is to consolidate all devices into a unified platform. This consolidation does not involve parsing configurations. Instead, it focuses on verifying communication between AppViewX and other devices. This setup lays the foundation for potential automation. In the future, direct communication can occur based on the provided credentials, enabling streamlined and efficient automation processes.

1. Go to **Menu** > **FIREWALL+** > **DEVICE MANAGEMENT** > **Inventory**> **Firewall**.
   By default, the **Firewall** tab opens.
2. Click **Others** tab from the home page.



3. Enter or select the field information in the **General Information** section.

Field and Description Table

Field	Description
Device name	Name of the device.
IP address	Enter the IP address.
Port	Enter the valid port number.
Model	Enter the model number.
Description	Enter the details.
Data center	The data center on which the device has been hosted. Select a Datacenter from the drop-down list or enter a data center name.

Field	Description
***IP address/ FQDN**	Enter the IP address or FQDN based on the selected communication mode.
Data center	Select from an existing list or enter a new data center.
**: Mandatory fields*	

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

Field and Description Table

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

5. Click **Save**

Note:

- To discard the changes, click the **Cancel** button.

Related information
Vendor Specific Discover/Onboard Firewall Device

Chapter 4: About Network Topology

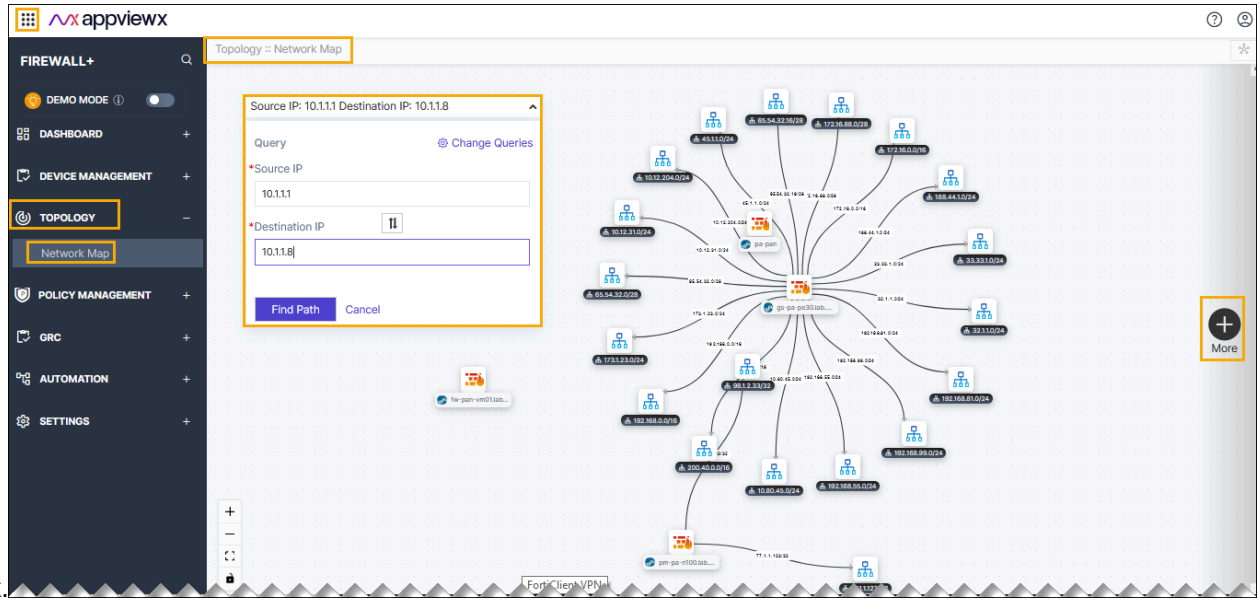
The Network Topology refers to the physical or logical arrangement of devices and connections in a network. The primary objective is to create a visual representation of the network topology, specifically focusing on managed firewalls, Application Delivery Controllers (ADCs), Layer 2 (L2) devices, Layer 3 (L3) devices, and routes. This graphical representation serves as a visual map of how these network components are interconnected, providing a clear and informative overview of the network's structure and configuration.

Benefits of network topology,

- **Network Topology Discovery**: The solution automatically identifies and maps various network elements within an organization's infrastructure. This includes critical components like routers, switches, firewalls, load balancers, and other network devices.
- **Application Connectivity Mapping**: It goes beyond hardware and also maps out the application connectivity requirements within the network. This means it can discover which applications and services are active in the environment and determine how they communicate with each other.
- **Impact Assessment**: This capability is crucial for assessing the potential consequences of making changes to firewall rules or modifying the network. It allows organizations to predict how such changes might affect the overall network and application connectivity.
- **Dependency Analysis**: The solution delves into the dependencies between various network components and applications. It helps organizations understand the intricate interrelationships between devices and services. This analysis is highly valuable for identifying potential bottlenecks, single points of failure, and security risks within the network.

This solution helps to network administrators and IT professionals, providing a comprehensive and visual understanding of their network infrastructure, application interactions, and potential vulnerabilities. It aids in making informed decisions, optimizing network performance,

and enhancing security by uncovering hidden risks and dependencies within the network.



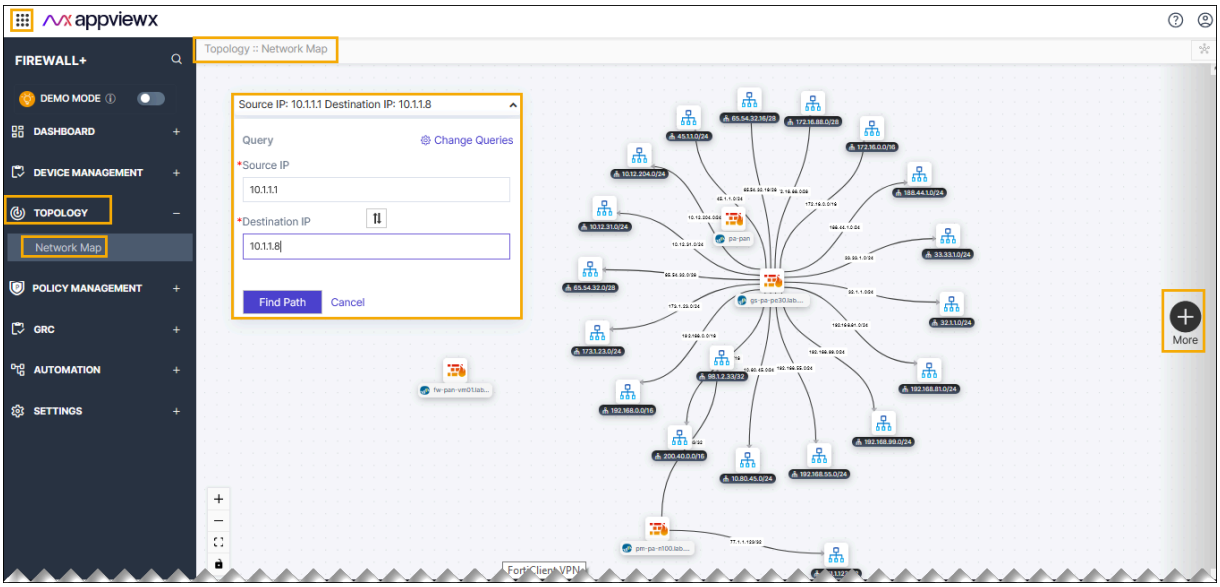
- Accessing the Network Topology

Accessing the Network Topology

To access the network topology, do the following steps.

1. Go to **Menu** > **FIREWALL+** > **TOPOLOGY** > **Network Map**.

   The **Network Map** page is displayed.



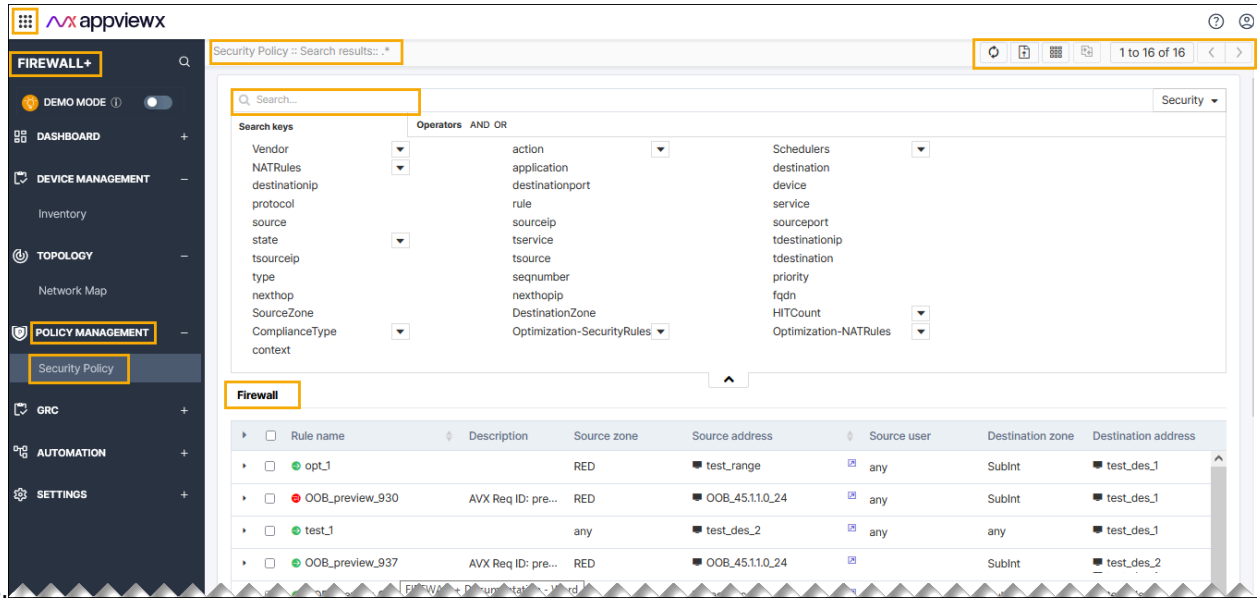
2. Click the IP drop-down menu, and then enter the Source IP and Destination IP in its field.
3. Click the **Find Path** button.

   Displays the different networks routes between the source and destination IPs.
4. To discard the search, click the **Cancel** button.

Chapter 5: Policy Management

Network security policy management is a process that aims to streamline the design and enforcement of security policies within a network. It involves the application of rules and best practices to manage firewalls and other network security devices more effectively, efficiently, and consistently. This helps organizations ensure that their network remains secure and compliant with their security requirements.

In AppViewX policy management, the application provides a visual representation of the roles and configurations of multi-vendor network devices. It consolidates all firewall vendors' rules into a single, unified interface. This means that you can view and manage the rules and policies of various firewall vendors in one centralized location, making it more efficient and user-friendly for administrators. This centralized approach simplifies the management of diverse firewall policies and enables a comprehensive view of network security configurations.



You can select the security rule you need directly from the security policy homepage. This suggests that within the security policy management system, you have the flexibility to choose and configure specific security rules as per your requirements without the need for navigating through complex menus or interfaces. This streamlined approach makes it easier to tailor security policies to your organization's needs and enhances overall usability.

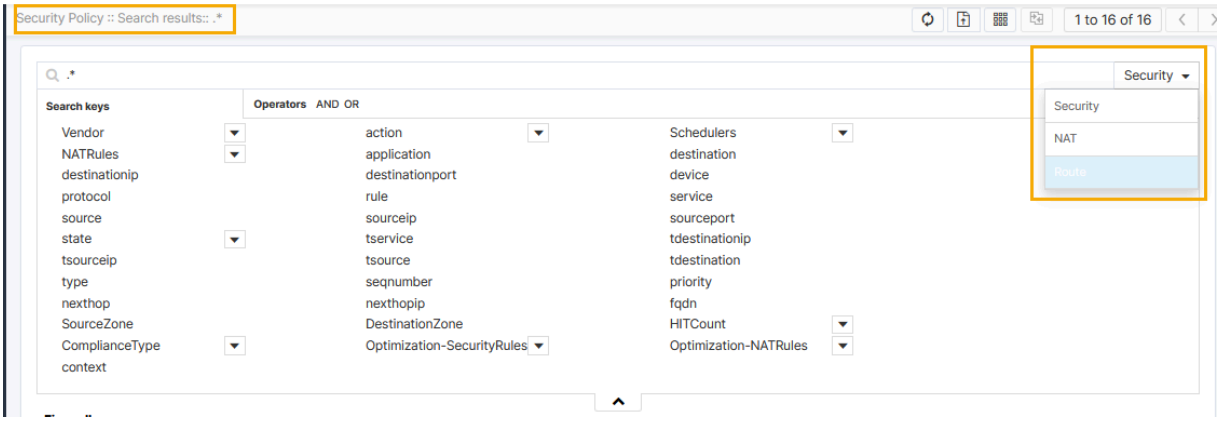
- Filtering the Rules
- Export Policy Details

Filtering the Rules

You have the capability to filter and display specific rules on the security policy homepage. This feature allows you to customize which security rules are visible, making it easier to focus on and manage the particular rules that are relevant to your current task or concern.

To filter the rule,

1. Go to **Menu** > **FIREWALL+** > **POLICY MANAGEMENT** > **Security Policy**.
   The security policy home page is displayed.



2. From the right-middle of the page, click the drop-down menu, and then select the required rule from the list.

Related information
Export Policy Details

Export Policy Details

The policy details, which are available in the Security Policy page can be exported into CSV or PDF file.

To export the details of one or more devices,

1. Go to **Menu** > **FIREWALL+** > **POLICY MANAGEMENT** > **Security Policy**.
2. If the device you want to export is not listed on the screen, run a search to locate it.
3. Click the  **Export** icon in the Command bar at the upper right of the screen.
4. On the **Export** pop-up screen that appears, select the type of file that you want to export in the Export poop-up window.
5. Click **Export**.
   The details are then downloaded as PDF or CSV file.

Related information
Filtering the Rules

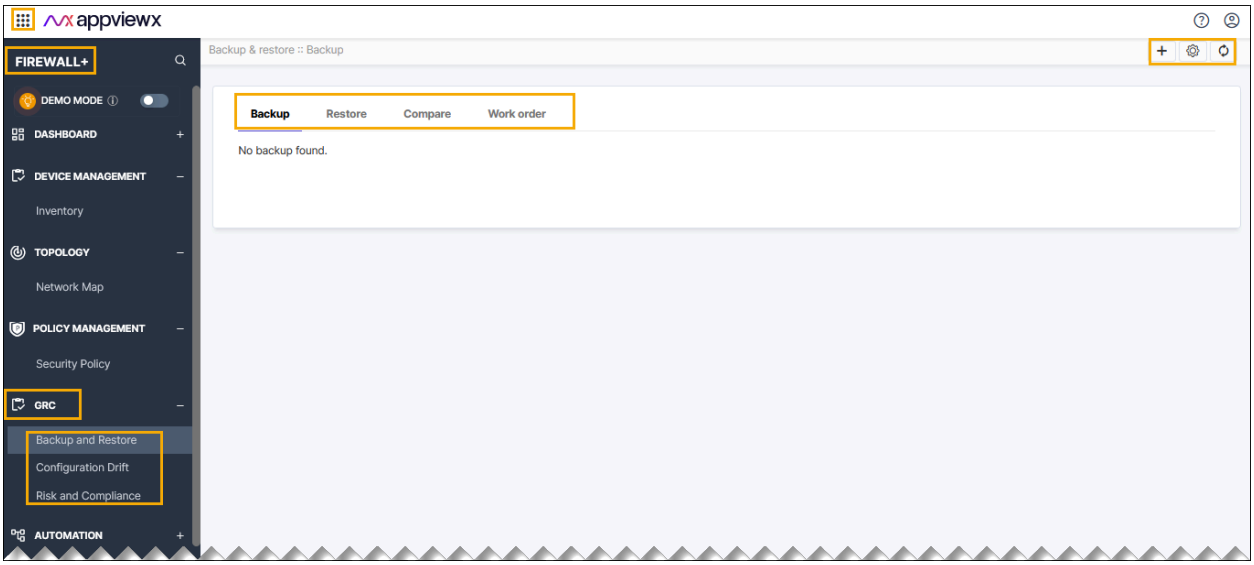
Chapter 6: GRC

About GRC

In the firewall solutions, Governance, Risk Management, and Compliance (GRC) encompasses a comprehensive set of practices. These practices involve the management of firewall policies and access controls in alignment with governance principles. They also focus on identifying and mitigating security risks and ensuring compliance with both industry regulations and organizational policies. The GRC within firewall solutions includes robust backup and restore functionalities, which serve to safeguard firewall configurations and policies. These features enable swift recovery in the face of failures or security incidents. This holistic approach seamlessly integrates security, governance, risk management, and compliance, all while providing the critical capability of data backup and restoration for firewall settings.

Firewall GRC encompasses the following key functionalities:

- Backup and Recovery
- Configuration Consistency Monitoring
- Risk Assessment and Compliance Management.



Benefits of Configuring Backup

- Ability to compare between two archives to see exactly what changes have taken place between the time frame of archive 1 (vs) archive 2.
- Essential details can be viewed and downloaded as pdf such as the files within the backup folder bigip, conf, etc. for your reference
- If the backup is scheduled on a regular basis, whatever misconfigurations or misbehavior of network outage or power failure on the device can be recovered and restored for valid configuration data.

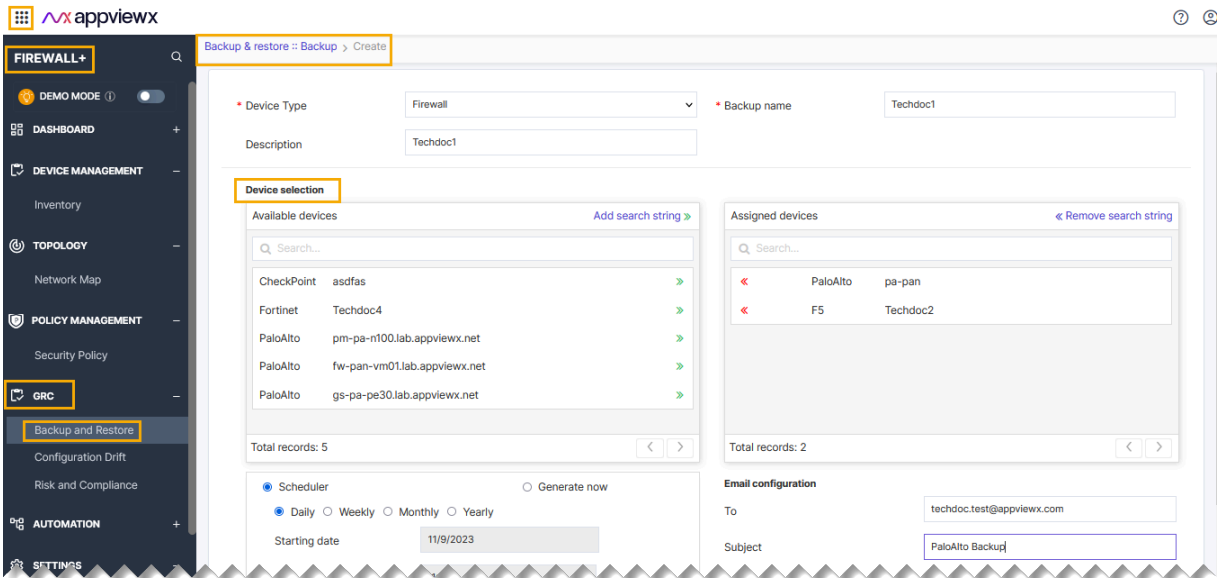
Related information
Creating a Device Backup
Deleting a Device Backup Group
Editing the Details of a Backup Group
Comparing the Device Backups
Restore and Rollback a Device
Risk and Compliance

Creating a Device Backup

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

To create a device backup group,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Backup and Restore**.
   The backup and restore home page is displayed.
2. Click the  (**Create**) icon from the left command bar.
   The backup page is displayed.



3. Select the **Device Type** from the drop-down list.
4. Enter the **Back name** in the field.
5. Enter a description of the name that makes it easy for users to determine what sort of device backups are found within the group.
6. In the Available devices field, click the » (**Assign item**) icon beside each device whose backups and restores you want to include.
7. 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.
8. In the **Email configuration** field, enter the email addresses, separated by commas, of all users who should be sent a copy of the backup.
9. (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 Firewall devices."
10. Click **Save**.

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

Related information
About GRC
Deleting a Device Backup Group
Editing the Details of a Backup Group
Comparing the Device Backups
Restore and Rollback a Device
Risk and Compliance

Deleting a Device Backup Group

To remove a device backup group from the AppViewX system,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Backup and Restore**.
   The backup and restore home page is displayed.
2. Click the  (**Delete**) icon against the device backup group that you want to delete.
   The Confirmation pop-up opens.
3. In the Confirmation pop-up, you have an option to enable Retain the generated backups. This option is enabled by default.

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

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

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

Related information
About GRC
Creating a Device Backup
Editing the Details of a Backup Group
Comparing the Device Backups
Restore and Rollback a Device
Risk and Compliance

Editing the Details of a Backup Group

To edit the details of a device backup group,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Backup and Restore**.
   The backup and restore home page is displayed.
2. In the list of backup groups on the screen, click the (**Edit**) icon for the device backup group you want to modify.
   The **Modify** screen opens.
3. In the **Modify** screen, update description, add/remove devices, change scheduler interval, and Email options.
4. Click **Save**.

Related information
About GRC
Creating a Device Backup
Deleting a Device Backup Group

Comparing the Device Backups

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

To compare backups for the same or different devices,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Configuration Drift**.
   The **Compare** tab opens.
2. On the **Compare** screen that opens, select the **Compare Type**: Device, Object, or Environment.
3. Select the Device names for which the configuration needs to be compared. The devices that have valid backups generated will be listed here.
4. In the **Device name** field, enter the name of the first device whose backup you want to compare.
5. In the **Archive 1** field, select the first backup in the comparison.
6. In the second **Device name** field, enter the name of the second device in the comparison. If you want to compare backups from the same device, enter the same name you entered in Step 4.
7. In the **Archive 2** field, select the second backup in the comparison.
8. Click **Compare**.
9. A table appears at the bottom of the screen, showing all of the files contained in the two backups you selected. The files are compared globally and a change summary is listed,

   - **Yellow** - Denotes the modifications
   - **Green** - Denotes the new additions
   - **Red** - Denotes the deletions

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

Related information
About GRC
Creating a Device Backup
Deleting a Device Backup Group
Editing the Details of a Backup Group
Restore and Rollback a Device
Risk and Compliance

Restore and Rollback a Device

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

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

To restore a device, complete the following steps:

1. Click **Menu** > **FIREWALL+** > **GRC** > **Configuration Drift**.
   The **Restore** tab opens.
2. Click the **Restore** tab.
3. Enter the **Device name**.
4. In the date range field that appears below the **Device name** field, click the date you want to restore the device or object to.
5. Leave the default value in the **Restore to** field.
6. Click **Proceed**.
7. The screen refreshes and displays a Configuration in the latest archive field, which should show the backup you selected. The table below shows all of the files contained in the backup and displays yellow circles beside each file that has been modified since the backup was taken and red circles beside each file that has been removed since the backup date.
8. At the bottom of the screen, enter a reason for restoring to the backup.
9. Click **Restore**.
10. Validate the changes against the latest backup and the configuration that is going to be restored. Enter a reason for restore and proceed.
11. AppViewX will proceed with restoring the entire configuration file or the particular configuration of the objects in a step-by-step manner.
12. A Work Order ID will be generated to track the progress at anytime. (Track the IDs in the Work order tab)

13. During restoration, if AppViewX identifies any issues, an automatic configuration Rollback will be triggered, which can be tracked in the work order.
14. A manual Rollback can also be initiated on a need basis.

Related information
About GRC
Creating a Device Backup
Deleting a Device Backup Group
Editing the Details of a Backup Group
Comparing the Device Backups
Risk and Compliance

Risk and Compliance

To create a risk and compliance,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Risk and compliance**.
   The **Risk report setting** page is displayed.
2. Click the **Risk settings** tab from the right of the page.
3. Click the + (**Create**) icon from the Risk setting command bar.
   By default, the **Violation Definition** page is displayed.
4. Select the required radio button from the **Violation Definition** page.
5. Click **Save**.
6. Select the required check box button from the **Profile Association** page.
7. Click **Save**.
8. Click **Cancel** if you do not want to create.

Configuring the Compliance for the Device

To create a risk and compliance,

1. Click **Menu** > **FIREWALL+** > **GRC** > **Risk and compliance**.
   The **Risk report setting** page is displayed.
2. Click the **Compliance** tab from the right of the page.
3. Select the required radio button from the **Firewall rule compliance definition** page.
4. Click **Save**.
5. Select the **Reset** button for the default option in the page.
6. Click **Save**.
7. Click **Cancel** if you do not want to create.

Related information
About GRC
Creating a Device Backup
Deleting a Device Backup Group
Editing the Details of a Backup Group
Comparing the Device Backups
Restore and Rollback a Device

Chapter 7: Setting

Settings

Overview

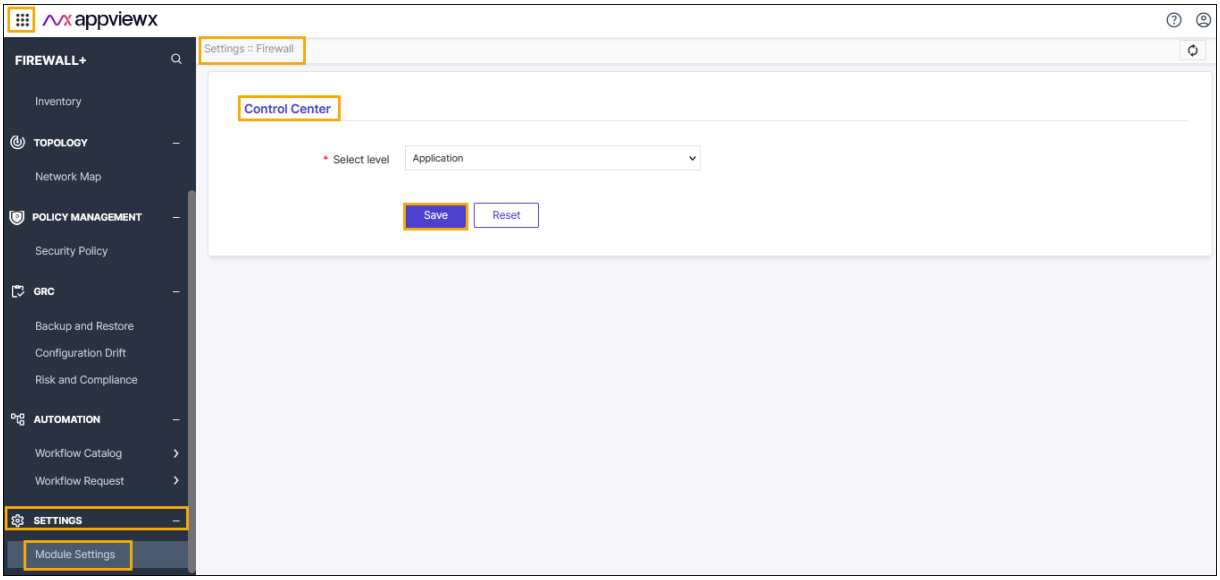
AppViewX's Firewall settings helps manage the Device and Object specifications related to Policy, Application, Device, and Context.

Configuring the Control Center

To configure the Control Center,

1. Click **Menu** > **FIREWALL+** > **SETTINGS** > **Module Settings**.

   The **Control Center** page is displayed.



2. Click **Select level** drop-down menu, and then select the level from the list. The available levels are,
   - Policy
   - Application
   - Device
   - Context.

3. Click **Save**.

   The pop-up **Settings updated successfully** message is displayed.

4. Click **Reset** for the default option.