



Forescout

eyeExtend for Palo Alto Networks Next- Generation Firewall

Configuration Guide

Version 2.0



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-06-19 08:56

Table of Contents

About the Palo Alto Networks Next-Generation Firewall Integration	5
About Certification Compliance Mode	5
Use Cases	5
Dynamic Firewall Access Control Powered by Forescout Platform Policy Detections.....	5
About Forescout eyeExtend for Palo Alto Networks NGFW	6
How It Works	7
What to Do	8
Requirements.....	9
Forescout Requirements.....	9
Forescout eyeExtend (Extended Module) Licensing Requirements.....	9
Per-Appliance Licensing Mode	10
Flexx Licensing Mode	11
More License Information	12
Palo Alto Networks Next-Generation Firewall Requirements	12
Install the Module	12
Set Up Palo Alto Networks Next-Generation Firewall	13
Generate an API Key	13
Prepare Your Security Policy – Create a Dynamic Address Group	14
Configure the Module	15
Configure the Panorama Server.....	15
Edit a Panorama Server	19
Remove a Panorama Server.....	20
Configure Individual Firewalls	21
Edit a Firewall.....	24
Remove a Firewall	25
Test the Module Configuration	26
Create a HIP Data Policy Using a Template	27
How Endpoints Are Detected and Handled.....	31
Create Custom Next-Generation Firewall Policies	31
Actions	31
Palo Alto Networks NGFW Policy Actions	32
Firewall – Create App-ID	32
Firewall – Create Security Policy Rule	35
Firewall – Map IP to User-ID	36
Firewall – Send HIP Data	38
Firewall – Tag Endpoint.....	41

Panorama – Create App-ID	43
Panorama – Create Security Policy Rule.....	45
Panorama – Map IP to User-ID	47
Panorama – Tag Endpoint.....	48
Work with Palo Alto Networks NGFW	50
Best Practices	50
General Guidance	50
Access the Asset Inventory	51
Access the Home Tab.....	51
Additional Forescout Documentation.....	52
Documentation Downloads	52
Documentation Portal	53
Forescout Help Tools.....	53

About the Palo Alto Networks Next-Generation Firewall Integration

The Forescout platform integrates with Palo Alto Networks® Next-Generation Firewall (NGFW) to significantly magnify the power of the firewall by leveraging the network visibility, inspection, and enforcement capabilities provided by the Forescout platform.

The integration lets security teams:

- Enrich the process of identifying, analyzing, and controlling network threats
- Enforce user-based and role-based access in real-time
- Implement dynamic segmentation of endpoints based on endpoint classification
- Enhance the firewall as an identity-savvy security solution

To use the module, you should have a solid understanding of Palo Alto Networks Next-Generation Firewall concepts, functionality, and terminology, as well as understand how the Forescout platform policies and other basic features work.

About Certification Compliance Mode

Forescout eyeExtend for Palo Alto Networks NGFW supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Use Cases

This section describes use cases supported by Forescout eyeExtend for Palo Alto Networks NGFW. To understand how this module helps you achieve these goals, see [About Forescout eyeExtend for Palo Alto Networks NGFW](#).

Dynamic Firewall Access Control Powered by Forescout Platform Policy Detections

Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, operating system, location, risk status, and more. This information is learned by Forescout platform policies and delivered to the firewall to deal with rapid network changes.

Critical HIP Data Without an Agent

Receive essential Host Information Profiles (HIP) from the Forescout platform, otherwise unavailable without the Palo Alto Networks GlobalProtect Agent installed on network endpoints.

Relying on the Forescout platform for this information ensures that remote endpoints and guests accessing your critical resources are adequately maintained and comply with security standards before they access your network.

Real-time Identity Information

Receive real-time mapping of the Forescout platform detected IP addresses to user IDs to support granular filtering of users rather than IP addresses. The Forescout platform-based IP address to User-ID capabilities provide vital support in environments where Active Directory is not available or limited.

Generate Firewall and App-ID Rules

Forescout dynamically generates firewall and App-ID rules in Panorama, as well as in specific firewalls. These rules can then be populated with new abilities referencing user identities to IP addresses, as well as Palo Alto tags. These functions can also be cancelled within the Forescout console.

Collectively, the goal of these features is to dramatically speed time to mitigation by automating the Palo Alto security infrastructure and making it significantly more accurate given the context of the Forescout platform.

About Forescout eyeExtend for Palo Alto Networks NGFW

Forescout eyeExtend for Palo Alto Networks NGFW lets you integrate the Forescout platform with Palo Alto Networks Next-Generation Firewall so that you can:

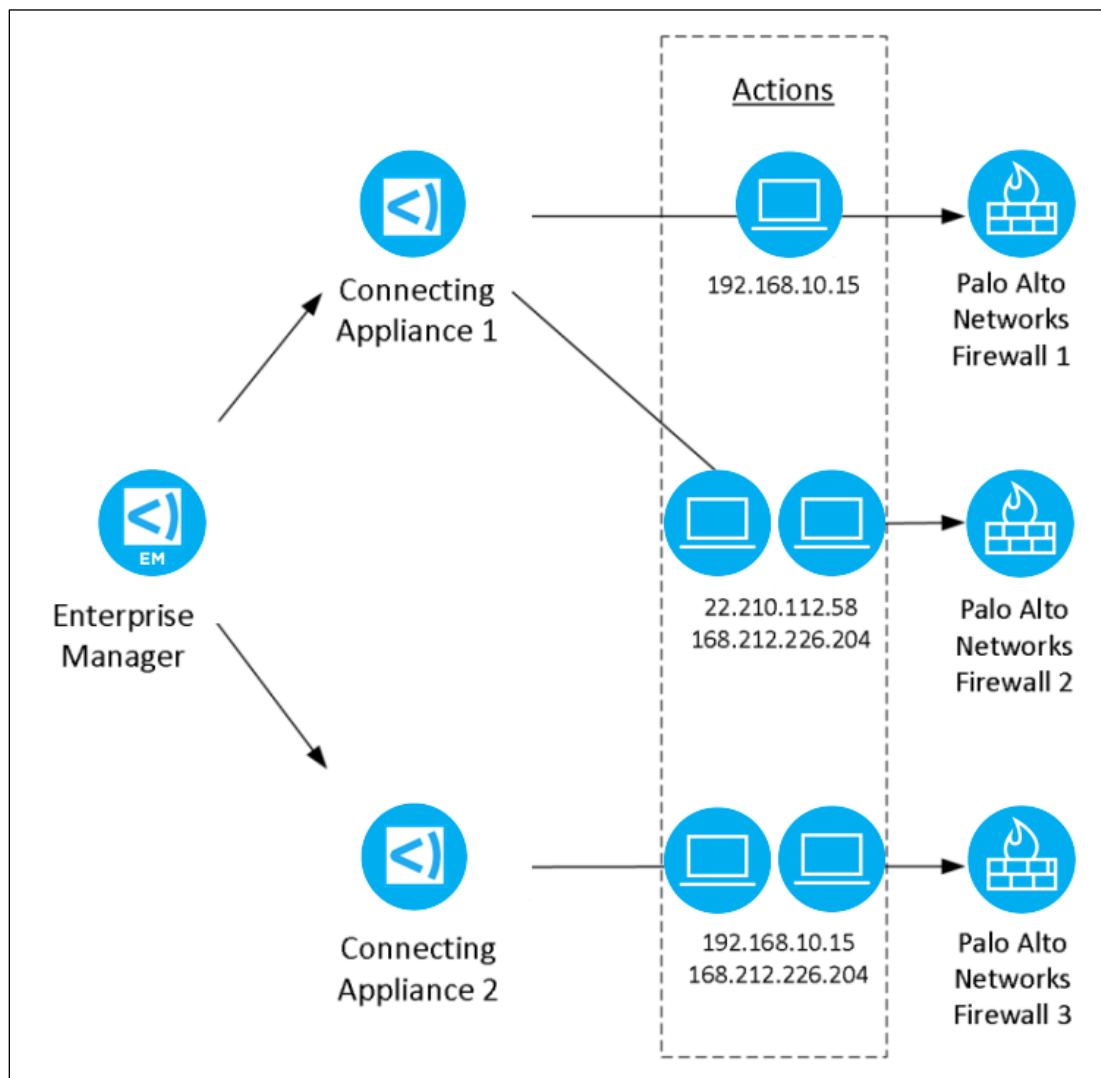
- **Enhance firewall access control capabilities by tagging endpoints**

You can leverage Palo Alto Network's use of tags as filtering criteria to determine the members of dynamic address groups. Using tags, the Forescout platform can dynamically add endpoints to Dynamic Address Groups based on endpoint assessment in policies. See [Firewall – Tag Endpoint](#) and [Panorama – Tag Endpoint](#).
- **Leverage the Forescout platform as a mission-critical real-time information source**
 - **Map endpoint IP addresses discovered by the Forescout platform to firewall or Panorama User-IDs.** For example, the module can map the IP address of a user authenticating to a captive portal through a proxy. This is particularly important in environments where the Palo Alto Global Connect client is absent or not fully deployed on all endpoints, so that firewall policies based on User-ID can remain effective in providing segmentation of traffic based on user groups. See [Firewall – Map IP to User-ID](#) and [Panorama – Map IP to User-ID](#).
 - **Send HIP (Host Information Profiles) data.** Use endpoint properties, discovered by the Forescout platform for policy enforcement, for example, domain name and operating system. See [Firewall – Send HIP Data](#).
- **Leverage dynamic generation of App-ID and policy rules in Panorama and in firewalls**
 - **Create an App-ID** and send it to Palo Alto Networks firewall(s) or to Panorama for deployment to the Palo Alto Networks firewall(s) that it manages. See [Firewall – Create App-ID](#) and [Panorama – Create App-ID](#).

- **Create a security policy rule** and add it to a Palo Alto Networks firewall or device group(s) on Panorama. See [Firewall – Create Security Policy Rule](#) and [Panorama – Create Security Policy Rule](#).

How It Works

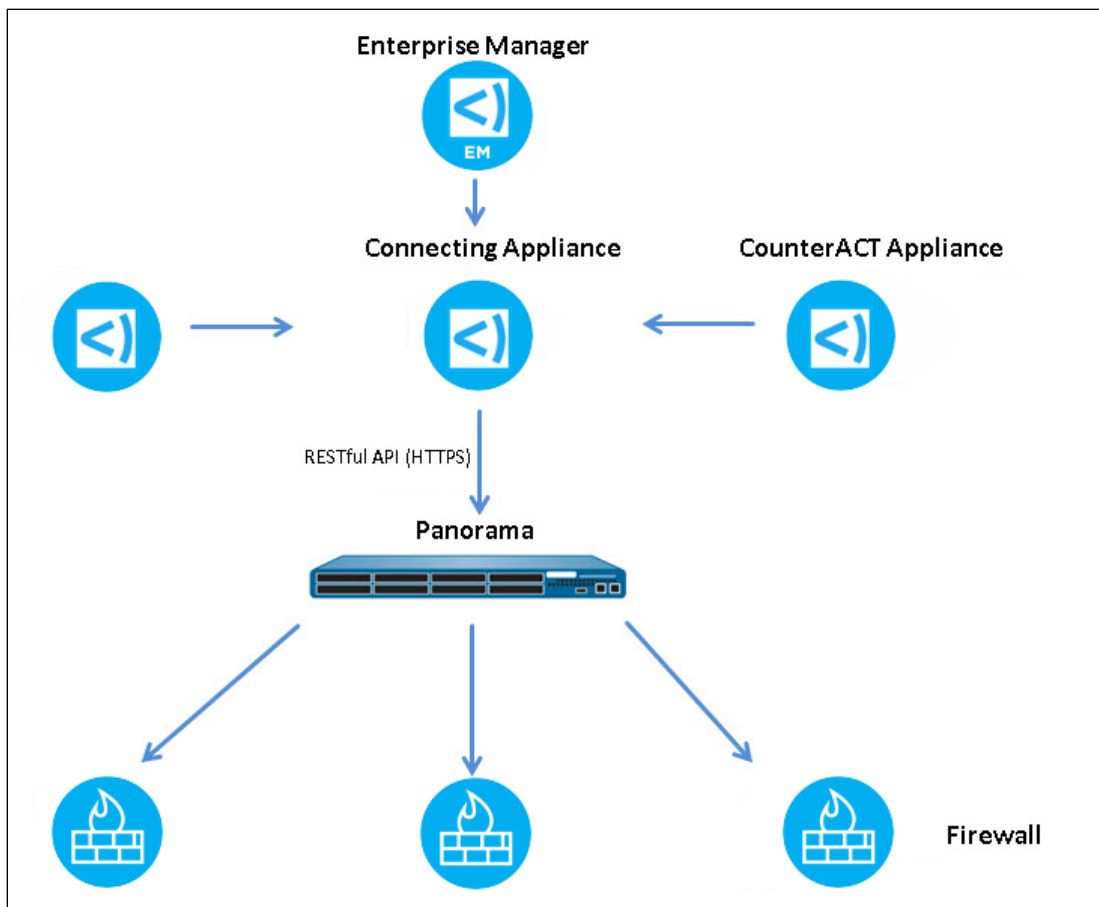
In addition to working directly with each firewall, Forescout eyeExtend for Palo Alto Networks NGFW integrates with the Palo Alto Network's central management system, Panorama, which manages a distributed network of virtual or physical firewalls.



The Forescout platform updates Panorama with endpoint tags so that firewalls can use these tags in real-time as matching criteria in the access rules.

Forescout eyeExtend for Palo Alto Networks NGFW communicates with Palo Alto Networks firewalls, supplying endpoint IP address information discovered by the Forescout platform through Firewall actions.

Each firewall is assigned to the connecting CounterACT® device with which it communicates. Multiple firewalls can be assigned to a single CounterACT device. The connecting CounterACT device then sends the action-related information to the relevant firewall.



The Forescout platform updates Panorama with endpoint tags so that firewalls can use these tags in real-time as matching criteria in the access rules.

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See [Requirements](#).
2. Review [Best Practices](#).
3. Download and install the module. See [Install the Module](#).
4. Configure settings in Palo Alto Networks Next-Generation Firewall. See [Set Up Palo Alto Networks Next-Generation Firewall](#).
5. Define Panorama details and module settings. See [Configure the Module](#).
6. Configure the Firewall and Panorama actions. See [Palo Alto Networks NGFW Policy Actions](#).

Requirements

Verify that the following requirements are met:

- [Forescout Requirements](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)
- [Palo Alto Networks Next-Generation Firewall Requirements](#)

Forescout Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.2.
- Content Module with the Windows Applications Plugin component running.
- Endpoint Module version 1.2, with the following components running:
 - HPS Inspection Engine
 - Linux
 - OS X
- A module license for Forescout eyeExtend for Palo Alto Networks Next-Generation Firewall. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).

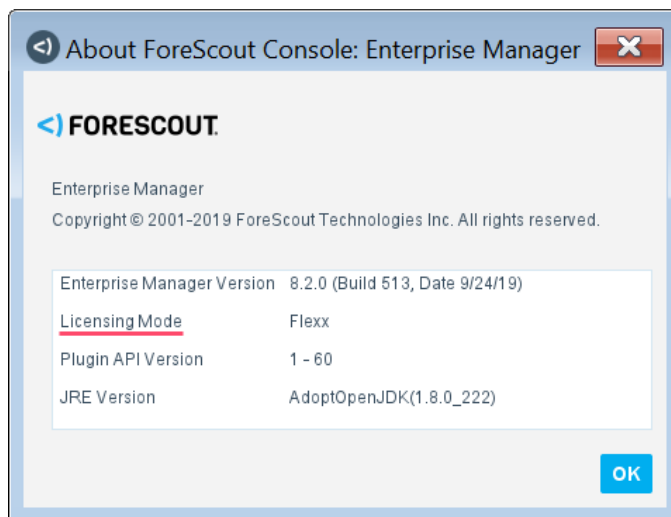
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Flexx Licensing Mode](#)

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.




Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

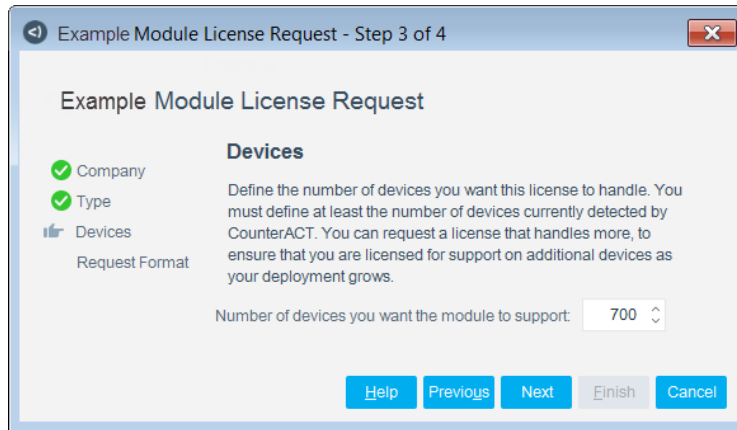
Demo license extension requests and permanent license requests are made from the Console.

 *This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.*

Requesting a License

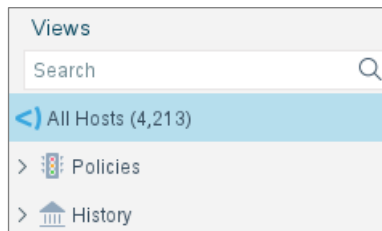
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.




To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend modules. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend modules. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

 *No demo license is automatically installed during system installation.*

License entitlements are managed in the [Forescout Customer Portal](#). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend modules, packaging individual licensed modules are supported. The eyeExtend Connect Module is an eyeExtend module even though it packages more than one module.

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the *Forescout Administration Guide*.
- **Flexx Licensing.** Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

Palo Alto Networks Next-Generation Firewall Requirements

- Palo Alto Networks Firewall running PAN-OS.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).
- For XML/REST API, ensure that you have the minimum requirements in the admin profile as indicated in green as follows:



Review Palo Alto Networks documents for how to create new administrators and admin profiles. Refer to <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin>.

Install the Module

This section describes how to install the module.


To install the module:


1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:

- [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
- [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

 *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

Set Up Palo Alto Networks Next-Generation Firewall

After you install the module, you need to:

- [Generate an API Key](#)
- [Prepare Your Security Policy – Create a Dynamic Address Group](#)

Generate an API Key

To access the Server API, the Forescout platform requires an API key. To generate this key, refer to the section about configuring an API key in the *PAN-OS Administrator's Guide*. This information is also available on the following website:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin>

Prepare Your Security Policy – Create a Dynamic Address Group

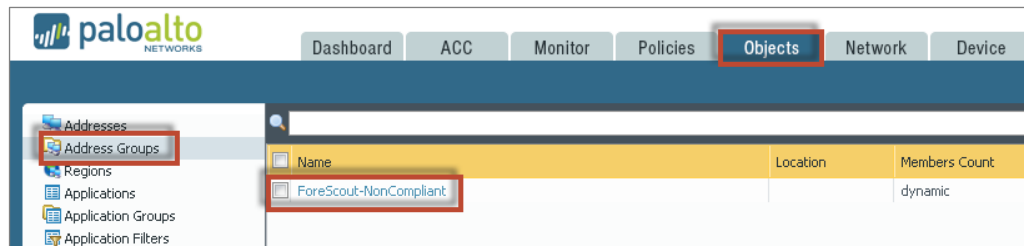
Dynamic Address Groups let you create a Forescout platform policy that automatically adapts to changes based on the filtering criteria of tags. These changes include additions, moves, or deletions of servers. It also provides flexibility for applying different rules to the same server based on its role on the network or the different kinds of traffic it processes.

To configure a Dynamic Address Group:

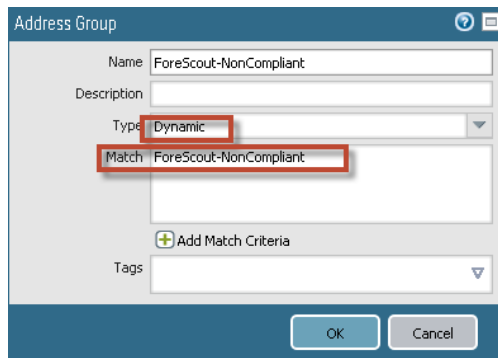
1. Log in to the web interface of the firewall.

Dynamic Address Groups to be used in this integration need to be created locally on the firewall. You cannot use Panorama shared objects.

2. Select the **Objects** tab and then select **Address Groups**.



3. Select **Add**.

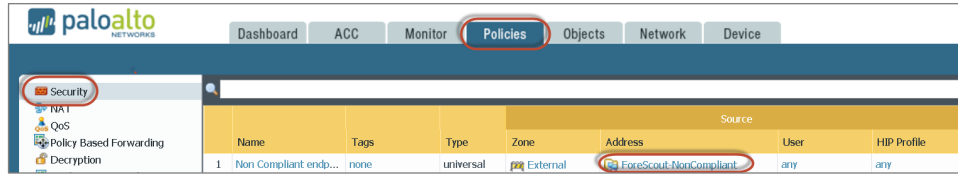


4. Give the Dynamic Address Group a name.
5. From the **Type** drop-down menu, select **Dynamic**.
6. Select **Add Match Criteria** and, as the tags are registered dynamically, add the match criteria in the **Match** field.

The Match Criteria you define will be available for selection in the Forescout action.

7. Select **OK** and then **Commit**.

You can now use the group in the firewall policy based on your security requirements.



Configure the Module

After Forescout eyeExtend for Palo Alto Networks NGFW is installed, configure the module to ensure that the Forescout platform can communicate with the Palo Alto Networks service as follows:

- Define the Panorama server, including the name of the server and the CounterACT device it communicates with, and then import the firewalls and device groups. See [Configure the Panorama Server](#).
- Define each firewall server and its login credentials, then import the tags and virtual systems. See [Configure Individual Firewall](#). This is only required for standalone servers.

Once configured, CounterACT devices synchronize with and provide information to these servers. Before you configure a firewall in the Forescout platform, you must ensure that the firewall has an administrator user with the required XML API permissions. See [Generate an API Key](#).

When restarting the module, you need to start and stop the module on all CounterACT devices at the same time. Do not restart the module on individual CounterACT devices.

Before configuring the module, review the [How It Works](#) section.

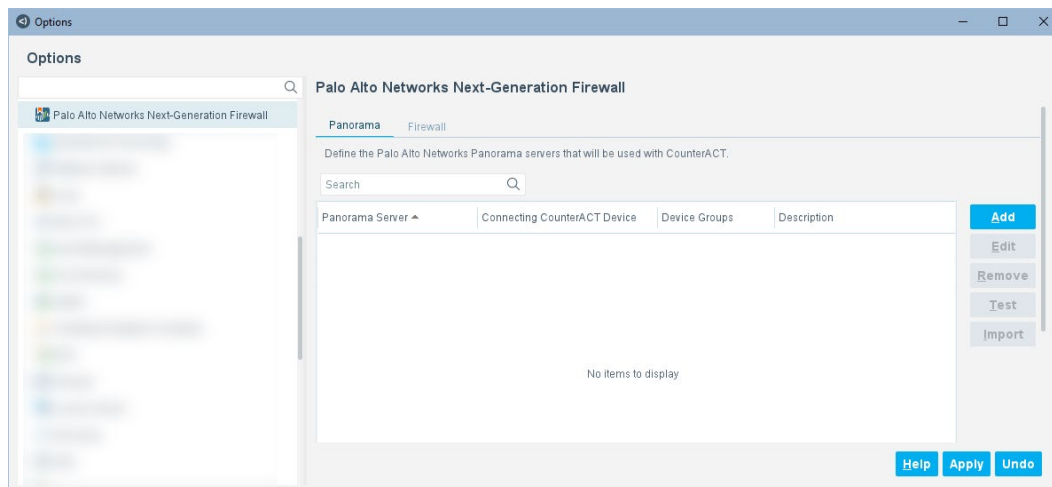
Configure the Panorama Server

Configure the Panorama server details and connecting CounterACT device.

To configure the Panorama Server:

1. Select **Options** from the **Tools** menu, and then select **Modules**.

2. In the Options pane, select **Palo Alto Networks Next-Generation Firewall**.




3. In the Palo Alto Networks Next-Generation Firewall pane, ensure that the Panorama tab is selected.
4. Select **Add**.

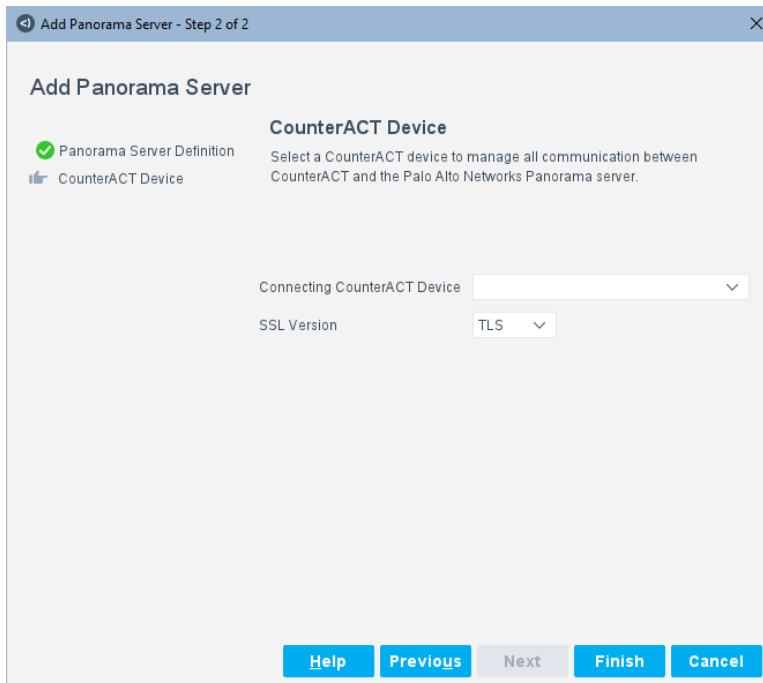
5. Configure the following connection parameters:

Panorama Server Name or IP Address	Enter the server name, a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the Panorama server.
Description	Enter a description of Panorama in the Forescout platform.

Server API Access Key	Enter the server API access key, required for API authentication.
Verify Key	Re-enter key to verify it.
Validate Server Certificate	<p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>

 When the Validate Server Certificate option is set in the Panorama Server Definition, the Firewall Definition inherits the same setting. However, if it is later changed in the Panorama Server Definition, that change is not reflected in the Firewall Definition. To update the Firewall Definition to match the Panorama Server Definition, import the firewalls. In the Palo Alto Networks Next-Generation Firewall pane, select the Panorama tab, select a Panorama server, and then select **Import**.

6. Select **Next**.



Add Panorama Server - Step 2 of 2

Add Panorama Server

☒ Panorama Server Definition
☐ CounterACT Device

CounterACT Device
 Select a CounterACT device to manage all communication between CounterACT and the Palo Alto Networks Panorama server.

Connecting CounterACT Device

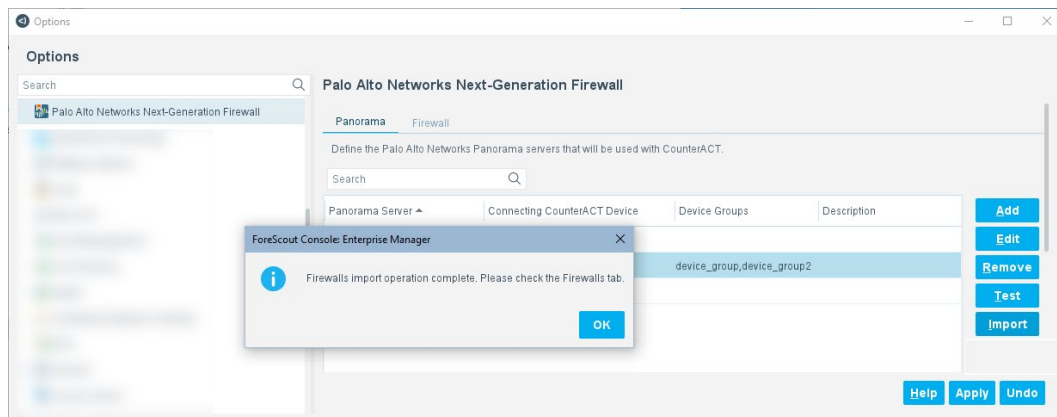
SSL Version

7. Configure the connecting CounterACT device:

Connecting CounterACT Device	Select the IP address of the CounterACT device that communicates with the firewall server. See Set Up Palo Alto Networks Next-Generation Firewall for details.
SSL Version	<p>Select the SSL version:</p> <ul style="list-style-type: none"> ▪ SSL – Select the preferred secured communication version to use. ▪ TLSv1.2 – Select this option if you are using PAN-OS 8.0.x. <p>Make sure the selected version is the same as configured on the firewall server.</p>

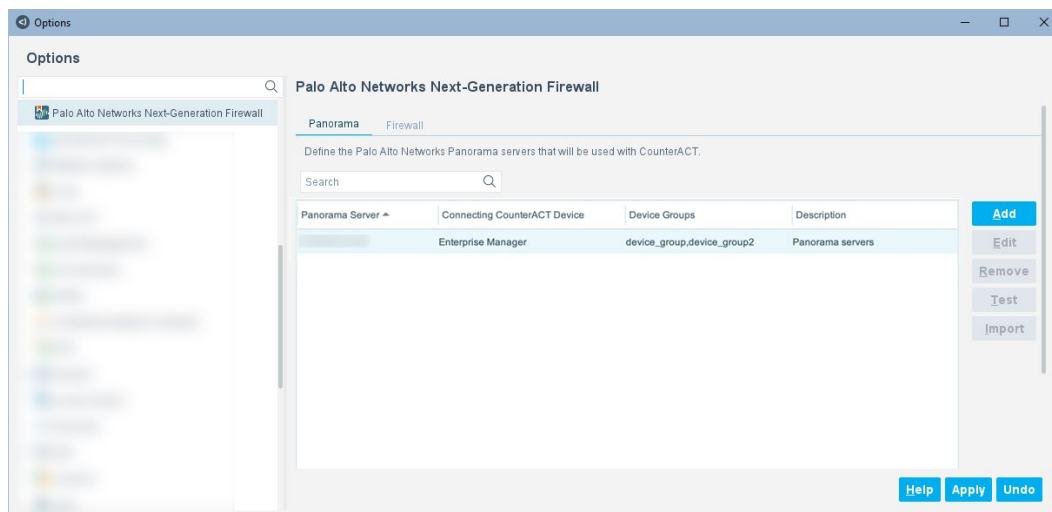
8. Select **Finish**. The new server is listed under the Panorama tab in the Palo Alto Networks Next-Generation Firewall pane.


9. If you have Palo Alto Networks firewalls that are managed by Panorama servers, select a server and then select **Import**.



The **Import** button on the Panorama tab imports Device Groups and managed firewalls that are properly connected (with a Device State on Panorama of **Connected**).

If there are any device group(s) defined on Panorama servers, they are displayed in the **Device Groups** column under the Panorama tab.



 You need to **Import** every time a new server is added to the Panorama Server and you want to add it to Forescout eyeExtend for Palo Alto Networks NGFW.

10. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

The best practice is to perform a test after setting up a connection. See [Test the Module Configuration](#).

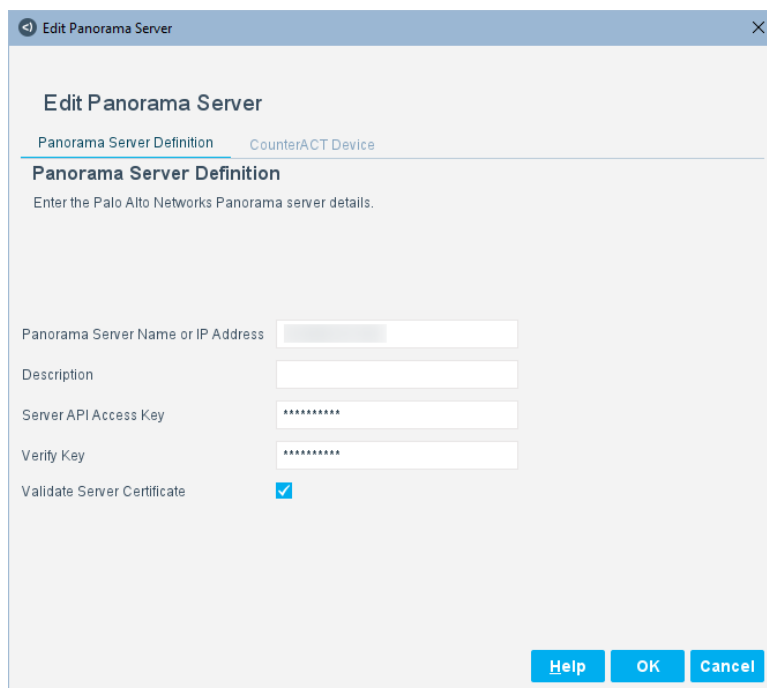
Edit a Panorama Server

Edit the Panorama server details and CounterACT device.

To edit a Panorama Server:

1. In the Palo Alto Networks Next-Generation Firewall pane, ensure that the Panorama tab is selected.

2. Select a Panorama Server and then select **Edit**.



3. Edit the connection parameters in the Panorama Server Definition and CounterACT Device tabs.
4. Select **OK**.
5. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

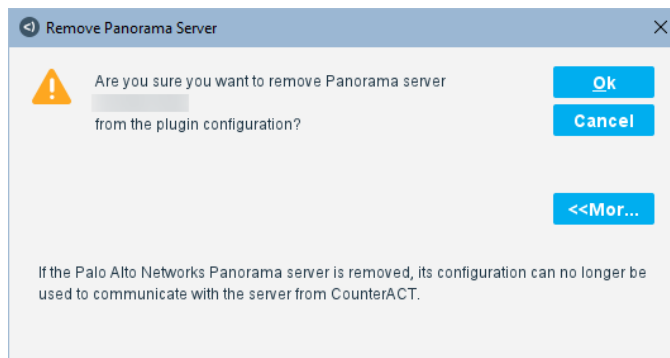
Remove a Panorama Server

Remove a Panorama server.

To remove a Panorama Server:

1. In the Palo Alto Networks Next-Generation Firewall pane, ensure that the Panorama tab is selected.
2. Select a Panorama Server and then select **Remove**.

3. For more information, select **More Info**.



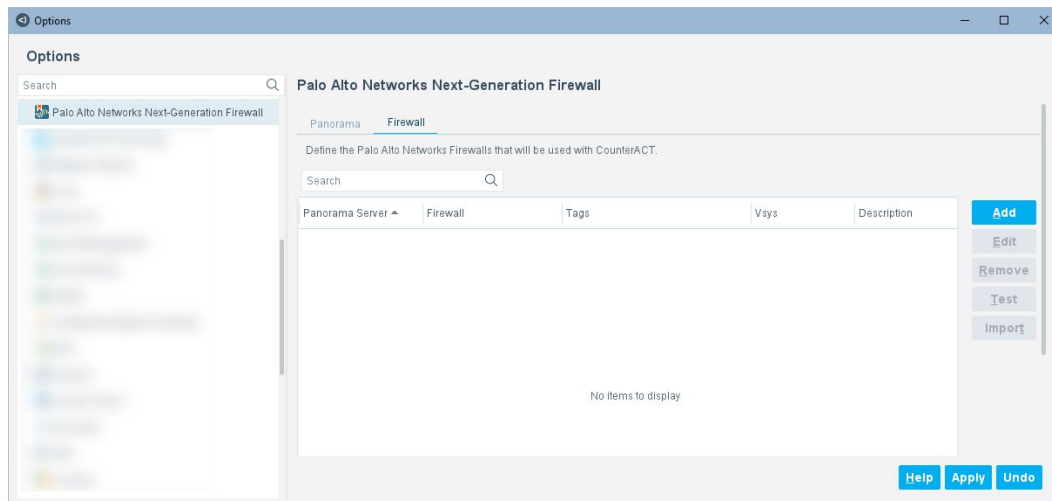
4. To confirm the removal, select **Ok**.
5. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

Configure Individual Firewalls

Configure individual firewall options to determine when API calls are sent from Forescout eyeExtend for Palo Alto Networks NGFW to the firewall.

To configure the firewall:

1. Select **Options** from the **Tools** menu, and then select **Modules**.
2. In the Options pane, select **Palo Alto Networks Next-Generation Firewall**, and select the Firewall tab.



3. Select **Add**.

Add Firewall

Firewall Definition
Enter the Palo Alto Networks Firewall details.

Firewall Name or IP Address

Firewall Vsys

Description

Server API Access Key

Verify Key

Validate Server Certificate ☒

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

4. Configure the following connection settings:

Firewall Name or IP Address	Enter the firewall name, a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the firewall.
Firewall Vsys	Enter the name of the virtual system (Vsys) within a physical firewall, for example, vsys1. To add multiple virtual systems within a single firewall, enter multiple Vsys names in the field, for example: vsys1, vsys2. Note that there are two types of firewall: Firewall VM and Physical Firewall. Firewall VM can have only one Vsys (vsys1) as a default whereas Physical Firewall can have multiple vsys.
Description	Enter a description of the firewall.
Server API Access Key	Enter the server API access key, required for API authentication.
Verify Key	Re-enter the key to verify it.

Validate Server Certificate

Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:

- Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance
- Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance

Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*.

5. Select Next.

The screenshot shows a configuration window titled "Add Firewall - Step 2 of 2". Inside, there's a section for "CounterACT Device" with instructions: "Select a CounterACT device to manage all communication between CounterACT and the Palo Alto Networks Firewall." Below this, there are two dropdown menus: "Connecting CounterACT Device" and "SSL Version" (which is currently set to "TLS"). At the bottom of the window, there are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

6. Configure the connecting CounterACT device:**Connecting CounterACT Device**

Select the IP address of the CounterACT device to communicate with the firewall server. See [Set Up Palo Alto Networks Next-Generation Firewall](#) for details.

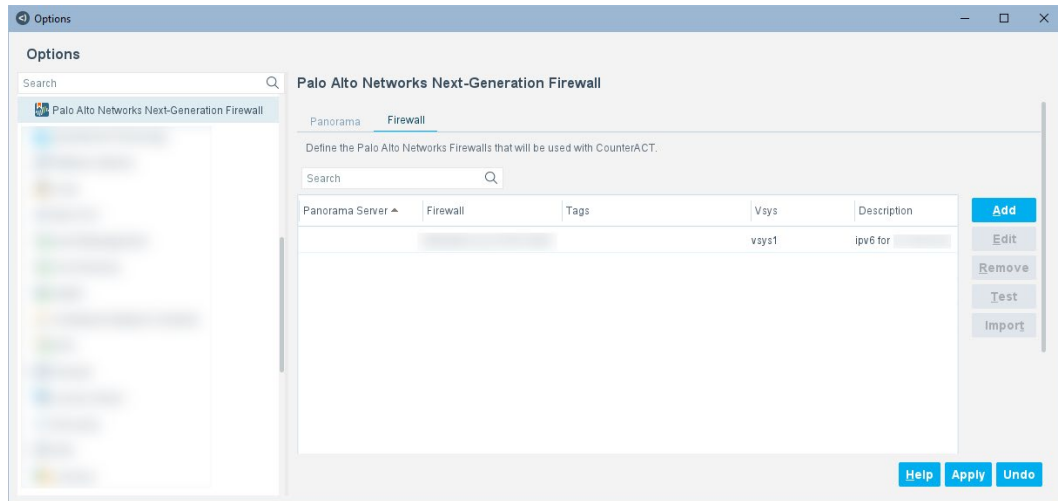
SSL Version

Select the SSL version:

- **SSL** – Select the preferred secured communication version to use.
- **TLSv1.2** – Select this option if you are using PAN-OS 8.0.x.

Make sure the selected version is the same as configured on the Palo Alto Panorama server.

7. Select **Finish**. The firewall is listed under the Firewall tab in the Palo Alto Networks Next-Generation Firewall pane. Virtual systems are displayed in the **Vsys** column.



8. To import tags related to a specific Firewall/vsys combination, select a Firewall and then select **Import**.

9. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

The best practice is to perform a test after setting up a connection. See [Test the Module Configuration](#).

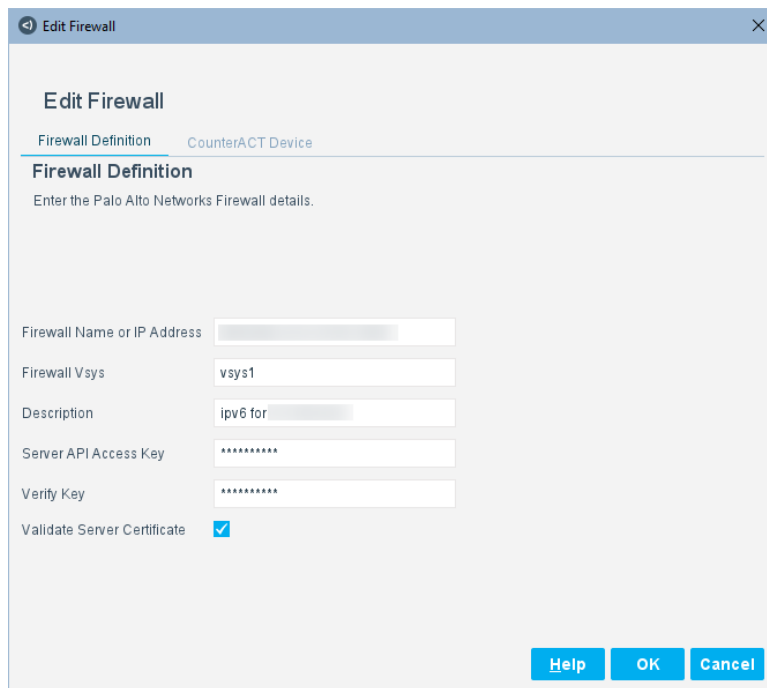
Edit a Firewall

Edit the firewall details and CounterACT device.


To edit a firewall:

1. In the Palo Alto Networks Next-Generation Firewall pane, select the Firewall tab.

2. Select a firewall and then select **Edit**.



3. Edit the connection parameters in the Firewall Definition and CounterACT Device tabs.

 When editing the **Firewall Vsys** name for an existing firewall device, specify only one Firewall Vsys name to modify.

4. Select **OK**.
5. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

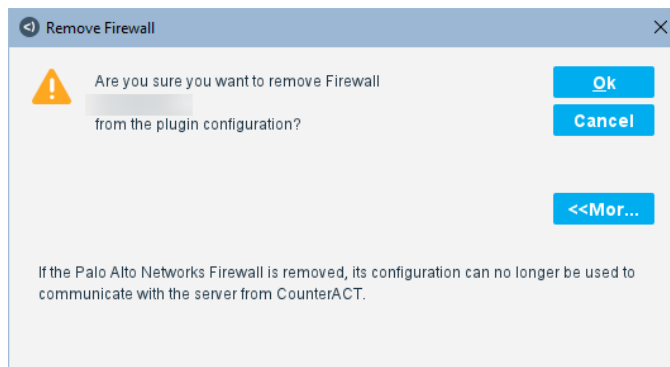
Remove a Firewall

Remove a firewall.

To remove a firewall:

1. In the Palo Alto Networks Next-Generation Firewall pane, select the Firewall tab.
2. Select a firewall and then select **Remove**.

3. For more information, select **More Info**.



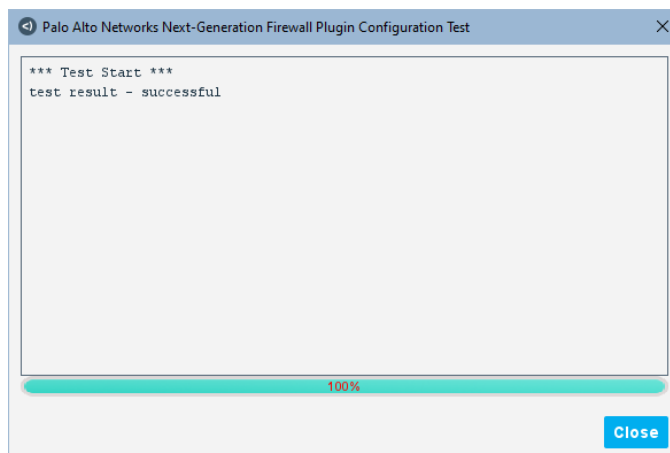
4. To confirm the removal, select **Ok**.
5. In the Palo Alto Networks Next-Generation Firewall pane, select **Apply**.

Test the Module Configuration

Perform a configuration test. The test checks the API connectivity to the Panorama Server or Firewall Server.

To run a test:

1. In the Palo Alto Networks Next-Generation Firewall pane, select the Panorama tab or select an item in the Firewall tab.
2. Select **Test**.



3. After viewing the results, select **Close**.

Create a HIP Data Policy Using a Template

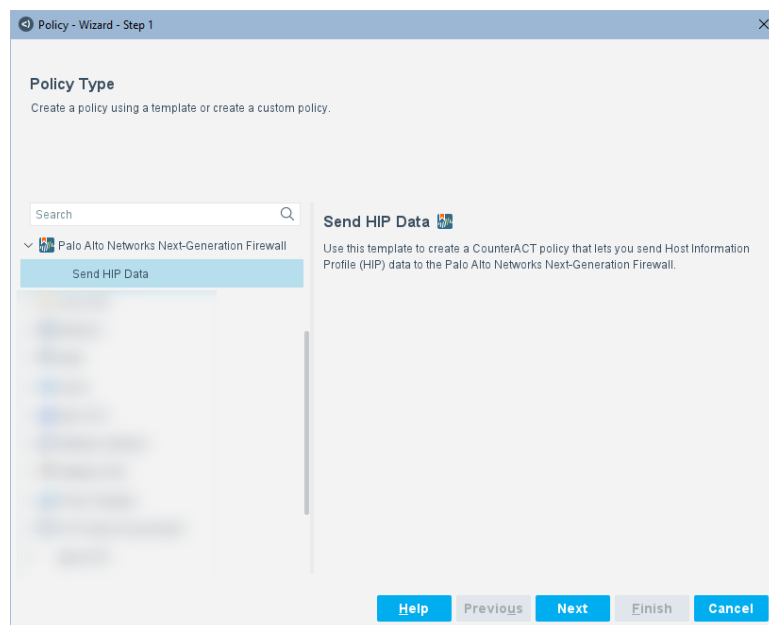
Forescout templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Predefined actions, which are instructions regarding how to handle endpoints, are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

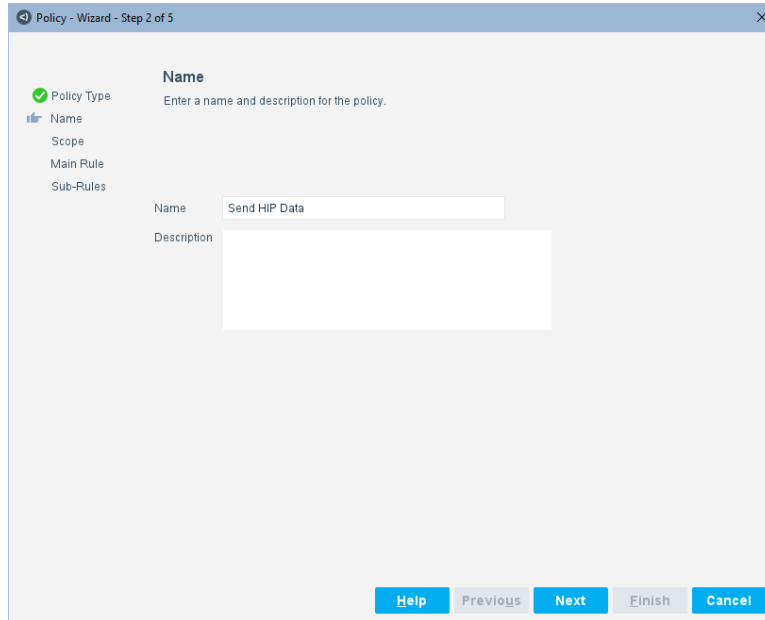
Use the Palo Alto Networks Next-Generation Firewall template to create a Forescout platform policy that lets you send Host Information Profile (HIP) data to the Palo Alto Networks Next-Generation Firewall.

To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager.
3. Expand the **Palo Alto Networks Next-Generation Firewall** folder and select **Send HIP Data**.



4. Select **Next**.



Policy Wizard - Step 2 of 5

Name
Enter a name and description for the policy.


Policy Type
Name
Scope
Main Rule
Sub-Rules

Name: Send HIP Data
Description:

Help Previous Next Finish Cancel

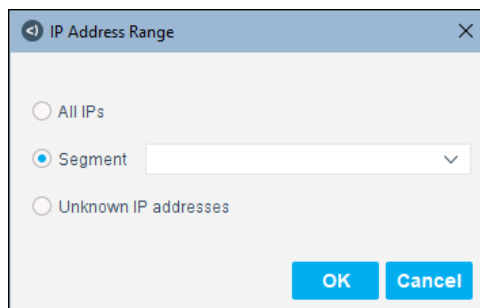
5. Define a unique name for the policy you are creating and enter a description.

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.



IP Address Range


☐ All IPs
☒ Segment
☐ Unknown IP addresses

OK Cancel

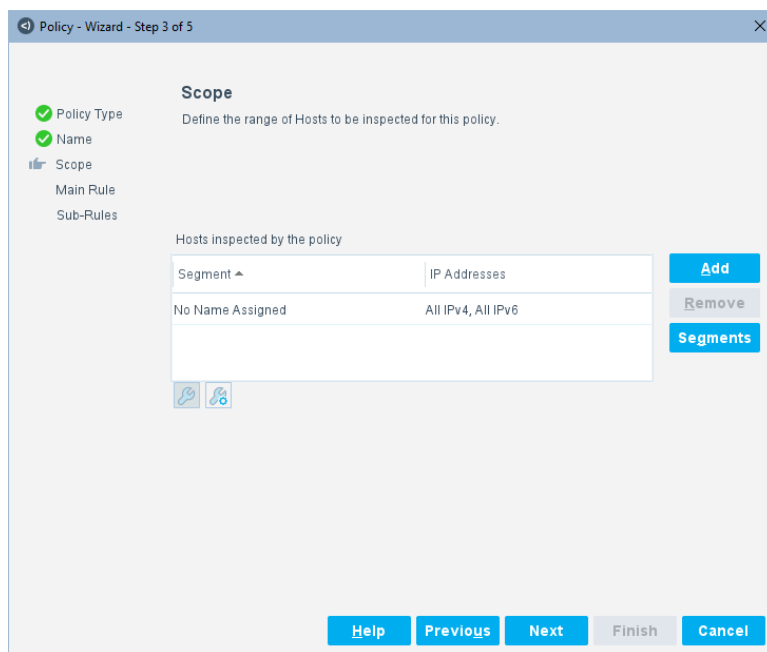
The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.

- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

 *Filter the range by including only specific groups and/or by excluding specific endpoints or users or groups when using this policy.*

8. Select **OK**. The added range is displayed in the Scope pane.



The screenshot shows the 'Policy - Wizard - Step 3 of 5' window. On the left, a sidebar lists configuration steps: Policy Type (checked), Name (checked), Scope (active), Main Rule, and Sub-Rules. The main area is titled 'Scope' with the instruction 'Define the range of Hosts to be inspected for this policy.' Below this, a table titled 'Hosts inspected by the policy' has two columns: 'Segment' and 'IP Addresses'. The first row shows 'No Name Assigned' and 'All IPv4, All IPv6'. To the right of the table are buttons for 'Add', 'Remove', and 'Segments'. At the bottom of the window are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

9. Select **Next**.

The main rule of this policy applies a filter to Windows, Linux, or Mac manageable devices. See [How Endpoints Are Detected and Handled](#).

10. Select **Next**.

Name	Conditions	Actions	Exceptions
1 Windows	Windows Manageable Domain: AND User: Any Value AND (NetBIOS Domain: Any Valu...		
2 Linux	(Linux Manageable (SecureConnector): OR Linux Manageable (SSH Direct Access):) ...		
3 Mac	(Macintosh Manageable (SecureConnector): OR Macintosh Manageable (SSH Direct Ac...		

A policy sub-rule is created for each Windows, Linux, or Mac device. For example, a Windows sub-rule not only checks whether the device is manageable but gets all the properties that can be sent as HIP data to the Palo Alto Networks firewall, such as user, domain, OS, AV enable status, and patch enable status. The action then sends whatever property is available to the Palo Alto Networks firewall. The sub-rules for Linux and Mac are set up in a similar way.

By default, these actions are disabled.

11. Select **Finish** to create the policy.

12. In the Policy Manager, select **Apply** to save the policy.

How Endpoints Are Detected and Handled

Policy rules instruct the Forescout platform how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

Create Custom Next-Generation Firewall Policies

You can use Forescout platform policies to:

- Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, operating system, location, risk status, and more. This information is learned by Forescout platform policies and delivered to the firewall to deal with rapid network changes.
- Leverage the Forescout platform as a mission-critical, real-time information source

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct the Forescout platform to apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

Actions

Forescout platform policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to an isolated VLAN or send an email to the device user or IT team.

In addition to the bundled Forescout actions available for detecting and handling endpoints, you can work with Forescout platform actions to create custom policies. These items are available when you install the module.

For more information about working with policies, select **Help** from the Policy Wizard.

To create a custom policy:

1. Log in to the Console and select **Policy**.
2. Create or edit a policy.

Palo Alto Networks NGFW Policy Actions

This section describes the actions available when Forescout eyeExtend for Palo Alto Networks NGFW is installed.

To access Palo Alto Networks Next-Generation Firewall actions:

- In the Policy Actions dialog box, expand the Palo Alto Networks Next-Generation Firewall folder in the Actions tree.

The following actions are available:

- [Firewall – Create App-ID](#)
- [Firewall – Create Security Policy Rule](#)
- [Firewall – Map IP to User-ID](#)
- [Firewall – Send HIP Data](#)
- [Firewall – Tag Endpoint](#)
- [Panorama – Create App-ID](#)
- [Panorama – Create Security Policy Rule](#)
- [Panorama – Map IP to User-ID](#)
- [Panorama – Tag Endpoint](#)

Firewall – Create App-ID

This action creates an App-ID and sends it to Palo Alto Networks firewall(s). You can select one or more target firewall servers. If you do not want to send an App-ID object, clear the text field.

Action

Search

Palo Alto Networks Next-Generation Firewall

- Firewall - Create App-ID
- Firewall - Create Security Policy Rule
- Firewall - Map IP to User-ID
- Firewall - Send HIP Data
- Firewall - Tag Endpoint
- Panorama - Create App-ID
- Panorama - Create Security Policy Rule
- Panorama - Map IP to User-ID
- Panorama - Tag Endpoint

This action creates an AppID and send it to firewall. Select one or more target firewalls. Clear the text field, if you do not wish to send a particular AppID object.

Parameters **Schedule**

Name: {app_id_name}

Description: {app_id_desc}

Category: {app_id_category};{app_id_subcategory} ▾

Technology: {app_id_technology} ▾

Protocol: {app_id_protocol} ▾

Open Ports: {app_id_ports}

Risk Factor: {app_id_risk} ▾

Specify one or more Firewalls

☒ Send to all firewalls

☐ Send to specific firewalls ...

Tags: Add Tags

Help OK Cancel

The following parameters are available:

Name	Enter a name of a new custom application in the Palo Alto Networks firewall. You can specify the name in up to 31 characters. This name appears in the applications list when defining security policies.
Description	Enter the description for the custom application. Specify a description that will help other administrators understand the application you created.
Category	Select the application category and subcategory that are used to generate the Top Ten Application Categories chart and are available for filtering.
Technology	Select the technology for the application, for example, Client Server or Network Protocol .
Protocol	<p>Select the protocol for the application:</p> <ul style="list-style-type: none"> ▪ IP: Specify an IP protocol other than TCP or UDP ▪ ICMP: Specify an Internet Control Message Protocol version 4 (ICMP) type ▪ ICMP6: Specify an Internet Control Message Protocol version 6 (ICMPv6) type ▪ Port: Specify a port if the protocol used by the application is TCP and/or UDP ▪ None: Specify signatures that are independent of protocol
Open Ports	<p>Enter the open ports:</p> <ul style="list-style-type: none"> ▪ For Port, enter one or more combinations of the protocol and port number, one entry per line. The general format is: <protocol>/<port>. For example, TCP/dynamic or UDP/32. ▪ For IP, enter the protocol number from 1 to 255 ▪ For ICMP, enter the protocol number from 0 to 255 ▪ For ICMP6, enter the protocol number from 0 to 255

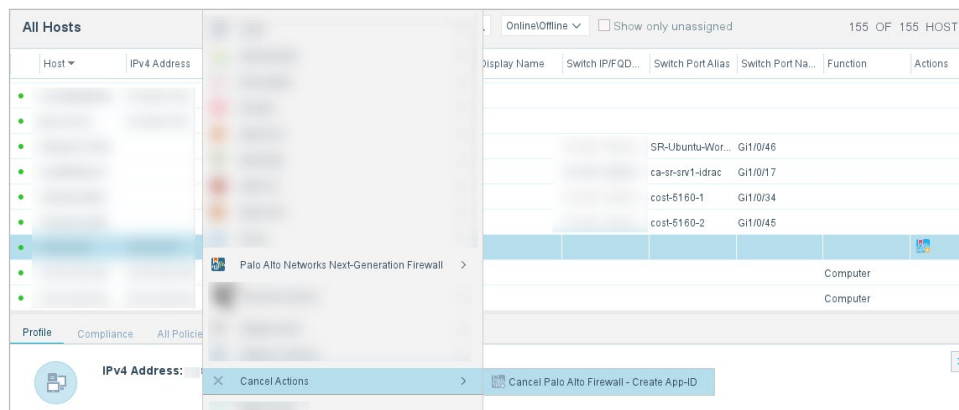
Risk Factor	Select the risk level associated with this application. Risk levels are from 1 to 5, with 1 being the lowest and 5 being the highest.
Specify one or more Firewalls	Specify one or more firewalls: <ul style="list-style-type: none"> ▪ Send to all firewalls: Create an App-ID and send it to all firewall servers. ▪ Send to specific firewalls: Create an App-ID and send it to selected firewalls only. Select one or more firewalls from the list of target firewall servers.
Tags	Select Add Tags to add tags to a selected field.

Cancel Firewall – Create App-ID

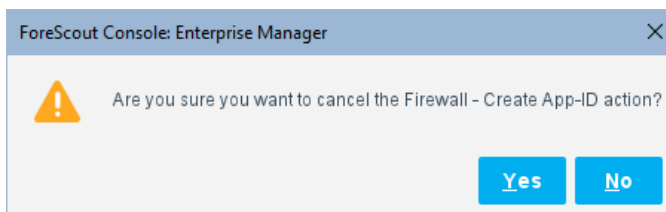
Cancel the Firewall – Create App-ID action.

To cancel the action:

1. In the **All Hosts** pane select an endpoint with the Firewall – Create App-ID action configured.
2. Right click, select **Cancel Actions**, and then select **Cancel Palo Alto Firewall – Create App-ID**.



A confirmation is displayed.



3. Select **Yes**.

Firewall – Create Security Policy Rule

This action adds a security policy rule to a Palo Alto Networks firewall.

The screenshot shows the 'Action' dialog box. On the left, a search bar is at the top. Below it, a tree view shows the following items: Palo Alto Networks Next-Generation Firewall, Firewall - Create App-ID, Firewall - Create Security Policy Rule (selected), Firewall - Map IP to User-ID, Firewall - Send HIP Data, Firewall - Tag Endpoint, Panorama - Create App-ID, Panorama - Create Security Policy Rule, Panorama - Map IP to User-ID, and Panorama - Tag Endpoint. The right pane has a title bar 'Action' and a close button. Below the title bar, it says 'This action adds a rule to the Firewall'. There are two tabs: 'Parameters' (active) and 'Schedule'. The 'Parameters' tab contains the following fields: Name, Description, From Zone, Source Address, To Zone, Destination Address, Application, and Service. Below these fields is an 'Action' dropdown menu set to 'Allow'. At the bottom, there are two radio buttons: 'Send to all firewalls' (selected) and 'Send to specific firewalls' (with a blue button next to it). At the bottom right, there are three buttons: 'Help', 'OK', and 'Cancel'.

The following parameters are available:

Name	Enter a name that identifies the rule. The name is case-sensitive and can be up to 63 characters. The name must be unique on a firewall.
Description	Enter a description for the policy in up to 1024 characters.
From Zone	Enter source zones. Zones must be of the same type (Layer 2, Layer 3, or virtual wire). The default is Any .
Source Address	Enter source addresses, address groups, or regions. The default is Any .
To Zone	Enter destination zones. Zones must be of the same type (Layer 2, Layer 3, or virtual wire). The default is Any .
Destination Address	Enter destination addresses, address groups, or regions. The default is Any .
Application	Enter specific applications for the security policy rule. If an application has multiple functions, you can select the overall application or individual functions.
Service	Select the services you want to limit to specific TCP or UDP port numbers.
Action	<p>Select the action the firewall takes on the traffic that matches the attributes defined in a rule:</p> <ul style="list-style-type: none"> ▪ Allow: Allows the matched traffic. This is the default. ▪ Deny: Blocks matched traffic and enforces the default Deny action defined for the application that is denied. ▪ Drop: Silently drops the application.

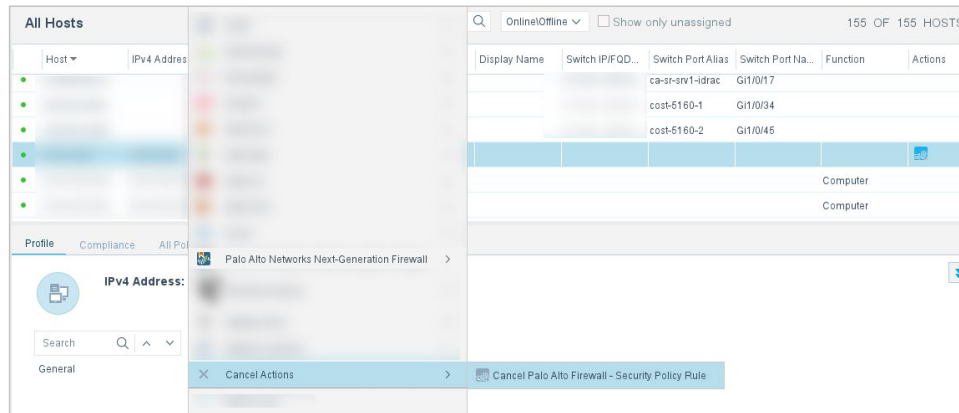
Specify one or more Firewalls	<p>Specify one or more firewalls:</p> <ul style="list-style-type: none"> ▪ Send to all firewalls: Create a rule and send it to all firewall servers. ▪ Send to specific firewalls: Create a rule and send it to selected firewalls only. Select one or more firewalls from the list of target firewall servers.
--------------------------------------	---

Cancel Firewall – Create Security Policy Rule

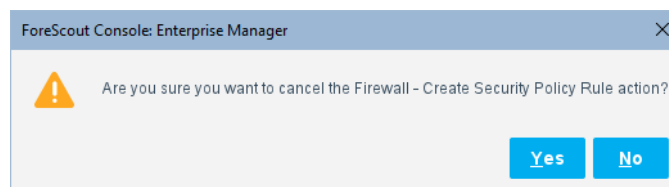
Cancel the Firewall – Create Security Policy Rule action.

To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Firewall – Create Security Policy Rule action configured.
2. Right click, select **Cancel Actions**, and then select **Cancel Palo Alto Firewall – Security Policy Rule**.



A confirmation is displayed.



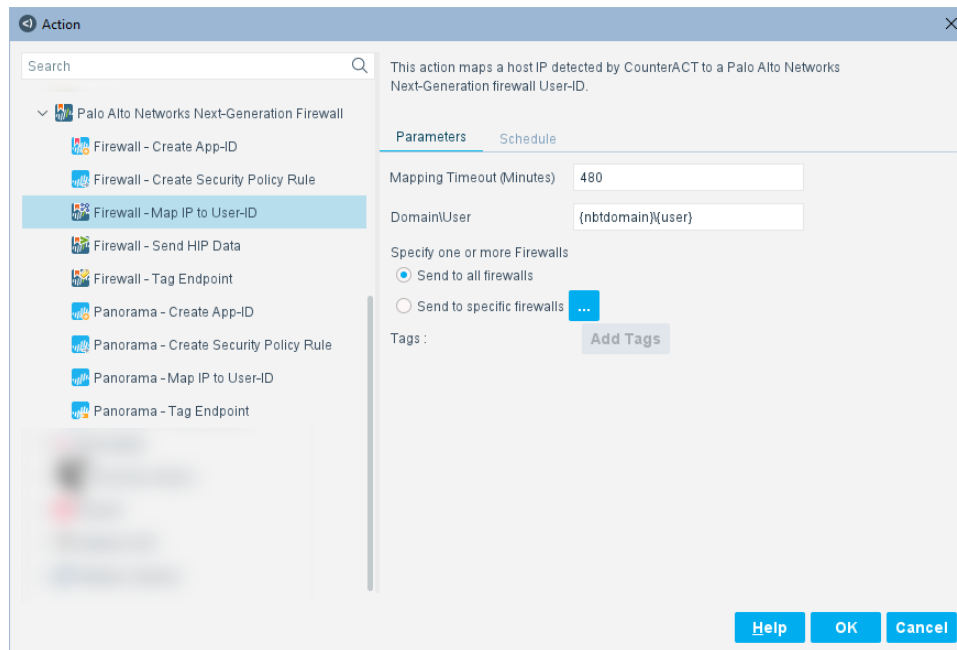
3. Select **Yes**.

Firewall – Map IP to User-ID

This action maps an endpoint IP address detected by the Forescout platform to a Palo Alto Networks NGFW firewall User-ID. The Forescout platform detects an FQDN to map an endpoint IP address.

The Palo Alto Networks NGFW employs a User Identification (User-ID) feature to configure and enforce firewall policies based on users. The User-ID identifies the user on the network and the IP addresses of the computers the user is logged into. In some situations, however, firewalls cannot easily map between an IP address and a

user identity. The module leverages the Forescout platform's advanced endpoint detection capabilities to identify and contribute user information to firewalls.



The following parameters are available:

Mapping Timeout (Minutes)	Enter the number of minutes that the action persists in the firewall. It is recommended to set a recurrence pattern to resend the User-ID/mapping data at an interval shorter than the timeout set in the action.
Domain\User	By default, this parameter consists of the <i>nbtdomain</i> and <i>user</i> property tags representing the NetBIOS domain and the username. You can select any property tag by using the Tags option.
Specify one or more Firewalls	Specify one or more firewalls: <ul style="list-style-type: none"> Send to all firewalls: Send to specific firewalls: The target firewall(s) to which the action is applied.
Tags	Select Add Tags to add tags to a selected field.

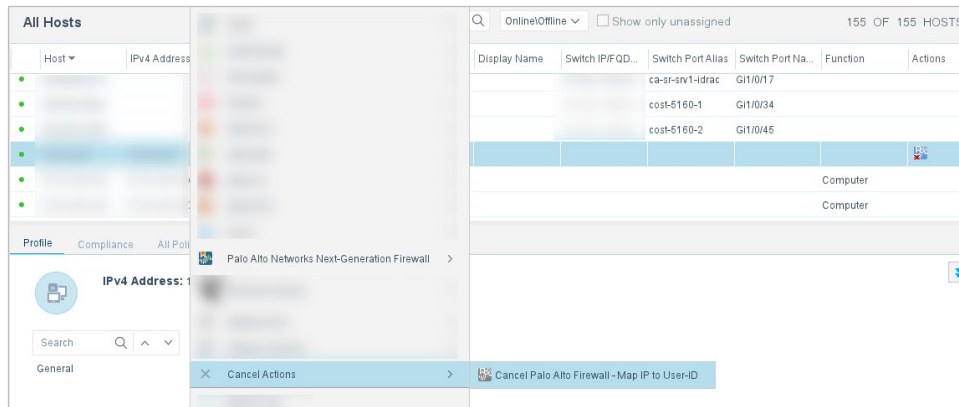
Cancel Firewall – Map IP to User-ID

Cancel the Firewall – Map IP to User-ID action.

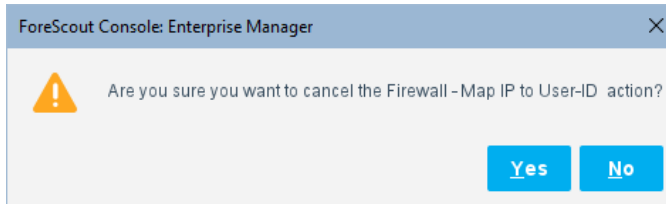
To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Firewall – Map IP to User-ID action configured.

2. Right click, select **Cancel Actions**, and then select **Cancel Palo Alto Firewall – Map IP to User-ID**.



A confirmation is displayed.



3. Select **Yes**.

Firewall – Send HIP Data

This action sends endpoint host properties that correspond to HIP data fields to the Palo Alto Networks firewall, where the information can be used to further filter access and create a more restrictive policy. This enables better security control.

Where Palo Alto segments or controls traffic based upon the compliance status of endpoints, the Forescout platform can provide timely information on compliance status through the sending of HIP data. HIP data can include data on running processes, encryption status, patch compliance, and antivirus status. This is particularly important in environments subject to regulatory requirements to block access of non-compliant endpoints to resources where sensitive personal, financial, or health information is stored.

This action reports the following information, if available:

- User, OS, Domain, and Hostname for Windows, Linux, or Mac devices
- Running process list for Windows, Linux or Mac devices
- Disk Encryption for Windows devices only
- Anti-virus, Firewall, and Patch Management enable/disable status for Windows and Mac devices

This action sends HIP data to firewall HIP objects. Select one or more target firewalls. If you do not want to send a particular HIP object, clear the text field.

This action sends HIP data to firewall HIP objects. Select one or more target firewalls. Clear the text field, if you do not wish to send a particular HIP object.

Parameters | **Schedule**

User: {user}

Domain: {nbtdomain}

OS: {user_def_fp}

OS Vendor: Irresolvable

Host Name: {nbthost}

Antivirus: {av_install}

Disk Encryption: {hd_installed_new}

Firewall: {fw_active}

Processes List: {process_no_ext}

Patch Management: {vulns}

Specify one or more Firewalls

☒ Send to all firewalls

☐ Send to specific firewalls ...

Tags : Add Tags

Help OK Cancel

Palo Alto Networks HIP objects are mapped to a CounterACT host property and the module that provides the host property.

The following parameters are available:

Parameter	OS	Data Sent	Default Forescout Platform Property	Dependency
User	Windows	Logged in User	{user}	HPS Inspection Engine
	Mac	Logged in User	{mac_logged_users}	Mac/Linux Property Scanner
	Linux	Logged in User	{linux_logged_users}	Mac/ Linux Property Scanner
Domain	Windows/ Mac/Linux	Domain	{nbtdomain}	Packet Engine
OS	Windows/ Mac/Linux	OS	{user_def_fp}	Packet Engine
OS Vendor	Windows/ Mac/Linux	Irresolvable by the Forescout platform		

Parameter	OS	Data Sent	Default ForeScout Platform Property	Dependency
Host Name	Windows/ Mac/Linux	Host Name	{nbthost}	Packet Engine
Antivirus	Windows	Antivirus enabled or not	{av_install}	HPS Inspection Engine
	Mac	Antivirus enabled or not	{mac_process_running}	Mac/Linux Property Scanner
Disk Encryption	Windows	List of disk encryption products/vendors installed on endpoint	{hd_installed_new}	HPS Inspection Engine
Firewall	Windows	Firewall enabled or not	{fw_active}	HPS Inspection Engine
	Mac	Firewall enabled or not	{mac_process_running}	Mac/Linux Property Scanner
Processes List	Windows	List of running processes	{process_no_ext}	HPS Inspection Engine
	Mac	List of running processes	{mac_process_running}	Mac/Linux property scanner
	Linux	List of running processes	{linux_processes_running}	Mac/Linux property scanner
Patch Management	Windows	List of missing patches	{vulns}	HPS Vulnerability DB/HPS Inspection Engine
	Mac	List of missing patches	{mac_software_updates}	Mac/Linux property scanner/HPS Vulnerability DB

Specify one or more firewalls and/or tags:

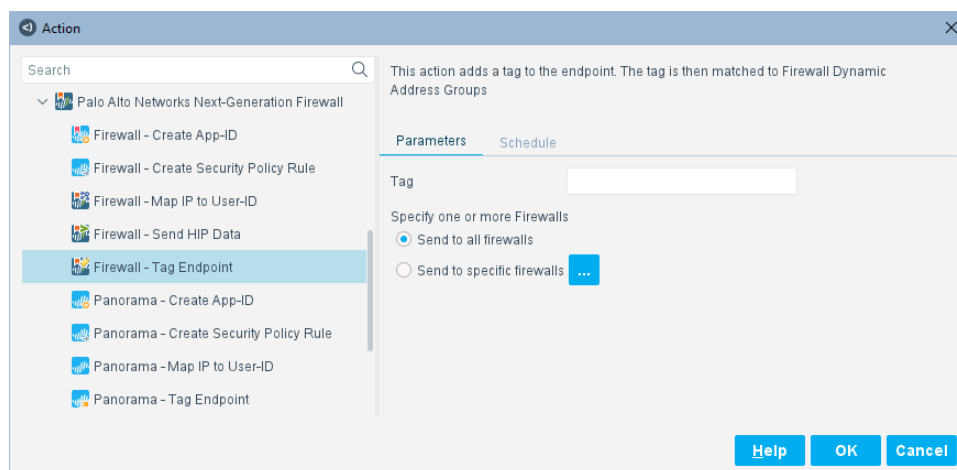
Specify one or more Firewalls	<p>Specify one or more firewalls:</p> <ul style="list-style-type: none"> ▪ Send to all firewalls: Sends HIP data to all firewall servers. ▪ Send to specific firewalls: Sends HIP data to selected firewalls only. Select one or more firewalls from the list of target firewall servers.
Tags	Select Add Tags to add tags to a selected field.

Firewall – Tag Endpoint

This action adds a tag to an endpoint. The tag is then matched to a Firewall Dynamic Address Group by the Palo Alto Networks firewall.

A tag is a string or attribute that the firewall uses to match and determine the members of the group of endpoints that it handles. The tag comprises logical *and* and *or* operators for defining the filtering criteria. The Forescout platform detects the endpoints to which these tag criteria are applied.

To ensure that you support the latest Dynamic Access Group configuration, ensure that you have imported the most recent tags set up on the server. See [Prepare Your Security Policy – Create a Dynamic Address Group](#).



The following parameters are available:

Tag	A tag defined on the firewall server in the Palo Alto Networks Next-Generation Firewall platform. Names are case sensitive.
Specify one or more Firewalls	Specify one or more firewalls: <ul style="list-style-type: none"> ▪ Send to all firewalls: Send to all firewall servers. ▪ Send to specific firewalls: Send to selected firewalls only. Select one or more firewalls from the list of target firewall servers.

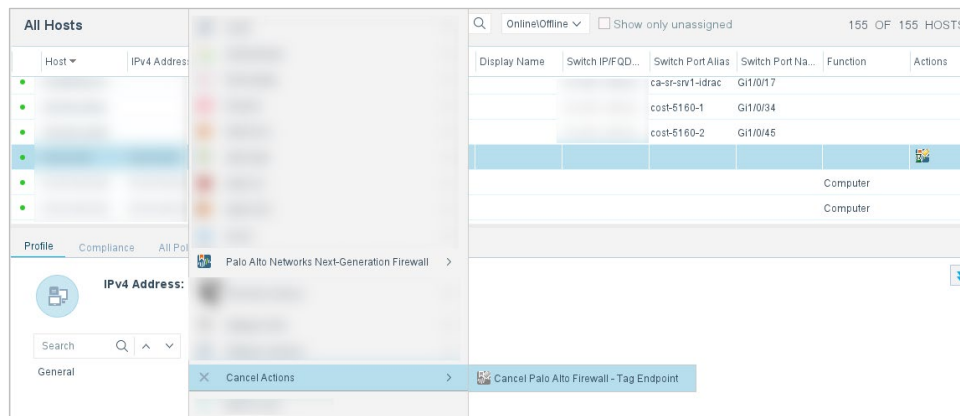
Cancel Firewall – Tag Endpoint

Cancel the Firewall – Tag Endpoint action.

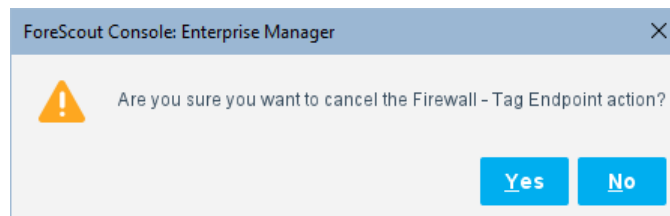
To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Firewall – Tag Endpoint action configured.

2. Right click, select **Cancel Actions**, and then select **Cancel Palo Alto Firewall – Tag Endpoint**.



A confirmation is displayed.



3. Select **Yes**.

Panorama – Create App-ID

This action creates an App-ID and sends it to Panorama for deployment to the Palo Alto Networks firewall(s) that it manages. You can select one or more target Panorama servers. If you do not want to send an App-ID object, clear the text field.

The following parameters are available:

Name	Enter a name of a new custom application in Panorama. You can specify the name in up to 31 characters. This name appears in the applications list when defining security policies.
Description	Enter the description for the custom application. Specify a description that will help other administrators understand the application you created.
Category	Select the application category and subcategory that are used to generate the Top Ten Application Categories chart and are available for filtering.
Technology	Select the technology for the application, for example, Client Server or Network Protocol .
Protocol	Select the protocol for the application: <ul style="list-style-type: none"> ▪ IP: Specify an IP protocol other than TCP or UDP ▪ ICMP: Specify an Internet Control Message Protocol version 4 (ICMP) type ▪ ICMP6: Specify an Internet Control Message Protocol version 6 (ICMPv6) type ▪ Port: Specify a port if the protocol used by the application is TCP and/or UDP ▪ None: Specify signatures that are independent of protocol

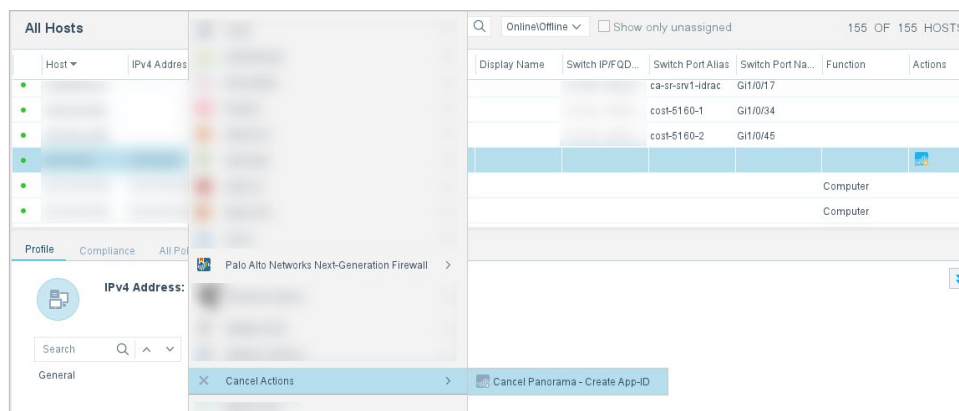
Open Ports	<p>Enter the open ports:</p> <ul style="list-style-type: none"> For Port, enter one or more combinations of the protocol and port number, one entry per line. The general format is: <protocol>/<port>. For example, TCP/dynamic or UDP/32. For IP, enter the protocol number from 1 to 255 For ICMP, enter the protocol number from 0 to 255 For ICMP6, enter the protocol number from 0 to 255
Risk	Select the risk level associated with this application. Risk levels are from 1 to 5, with 1 being the lowest and 5 being the highest.
Specify one or more Panoramas	Specify a specific Panorama Server/Device Group or Select All to select all Panorama Servers/Device Groups.

Cancel Panorama – Create App-ID

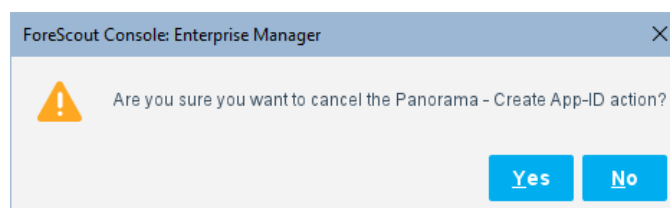
Cancel the Panorama – Create App-ID action.

To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Panorama – Create App-ID action configured.
2. Right click, select **Cancel Actions**, and then select **Cancel Panorama – Create App-ID**.



A confirmation is displayed.



3. Select **Yes**.

Panorama – Create Security Policy Rule

This action adds a security policy rule to device group(s) on Panorama.

Search

This action adds a rule to the Panorama

Parameters Schedule

Name

Description

From Zone

Source Address

To Zone

Destination Address

Application

Service

Action Allow

Specify one or more Panoramas

Search

✓ Panorama Server Device Groups

device_group

device_group2

Select All

Clear All

Help OK Cancel

The following parameters are available:

Name	Enter a name that identifies the rule. The name is case-sensitive and can be up to 63 characters. The name must be unique on a Panorama.
Description	Enter a description for the policy in up to 1024 characters.
From Zone	Enter source zones. Zones must be of the same type (Layer 2, Layer 3, or virtual wire). The default is Any .
Source Address	Enter source addresses, address groups, or regions. The default is Any .
To Zone	Enter destination zones. Zones must be of the same type (Layer 2, Layer 3, or virtual wire). The default is Any .
Destination Address	Enter destination addresses, address groups, or regions. The default is Any .
Application	Enter specific applications for the security policy rule. If an application has multiple functions, you can select the overall application or individual functions.
Service	Select the services you want to limit to specific TCP or UDP port numbers.

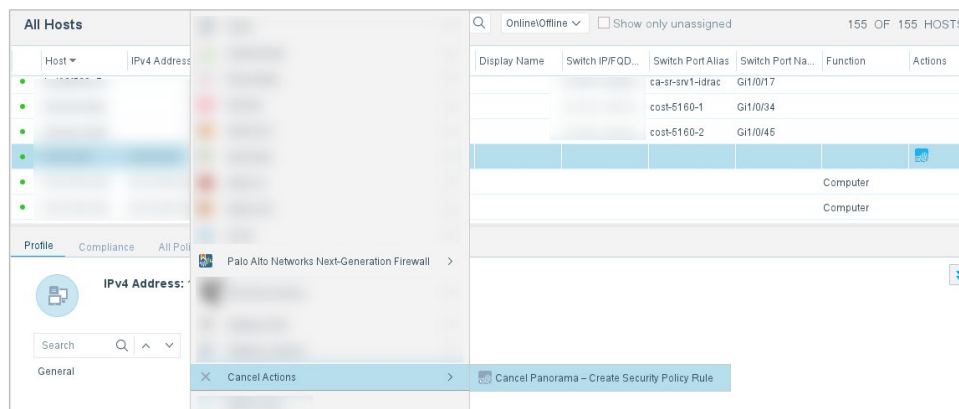
Action	<p>Select the action the Panorama takes on the traffic that matches the attributes defined in a rule:</p> <ul style="list-style-type: none"> ▪ Allow: Allows the matched traffic. This is the default. ▪ Deny: Blocks the matched traffic and enforces the default Deny action defined for the application that is denied. ▪ Drop: Silently drops the application.
Specify one or more Panoramas	Specify a specific Panorama Server/Device Group or Select All to select all Panorama Servers/Device Groups.

Cancel Panorama – Create Security Policy Rule

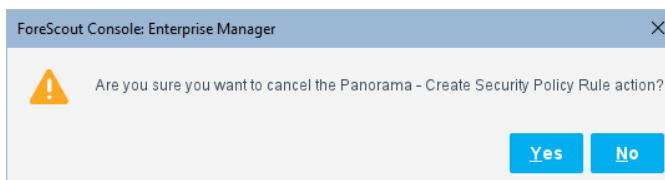
Cancel the Panorama – Create Security Policy Rule action.

To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Panorama – Create Security Policy Rule action configured.
2. Right click, select **Cancel Actions**, and then select **Cancel Panorama – Create Security Policy Rule**.



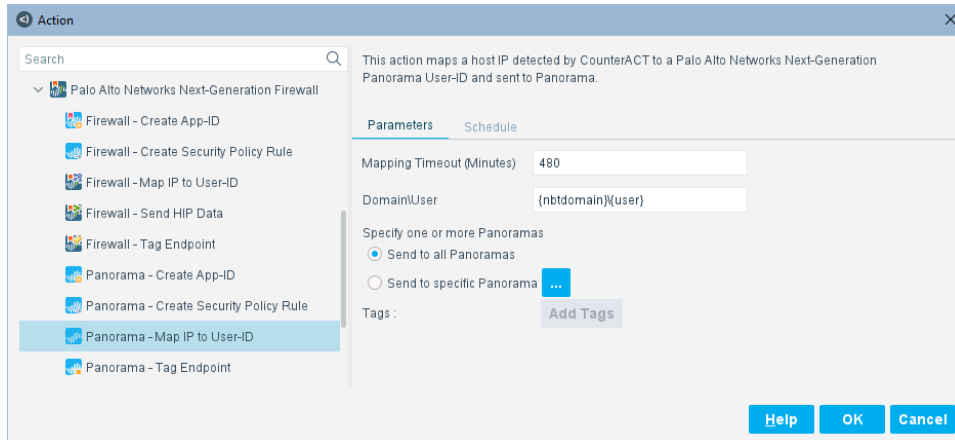
A confirmation is displayed.



3. Select **Yes**.

Panorama – Map IP to User-ID

This action maps an endpoint IP address detected by the Forescout platform to a Panorama User-ID and sends it to Panorama. The Forescout platform detects an FQDN to map an endpoint IP address.



The following parameters are available:

Mapping Timeout (Minutes)	Enter the number of minutes that the action persists in Panorama. It is recommended to set a recurrence pattern to resend the User-ID/mapping data at an interval shorter than the timeout set in the action.
Domain\User	By default, this parameter consists of the <i>nbtdomain</i> and <i>user</i> property tags representing the NetBIOS domain and the username. You can select any property tag by using the Tags option.
Specify one or more Panoramas	Specify one or more Panoramas: <ul style="list-style-type: none"> Send to all Panoramas: The action is applied to all Panorama servers. Send to specific Panoramas: The action is applied to selected Panorama(s). Select one or more Panorama(s) from the list of target Panorama servers.
Tags	Select Add Tags to add tags to a selected field.

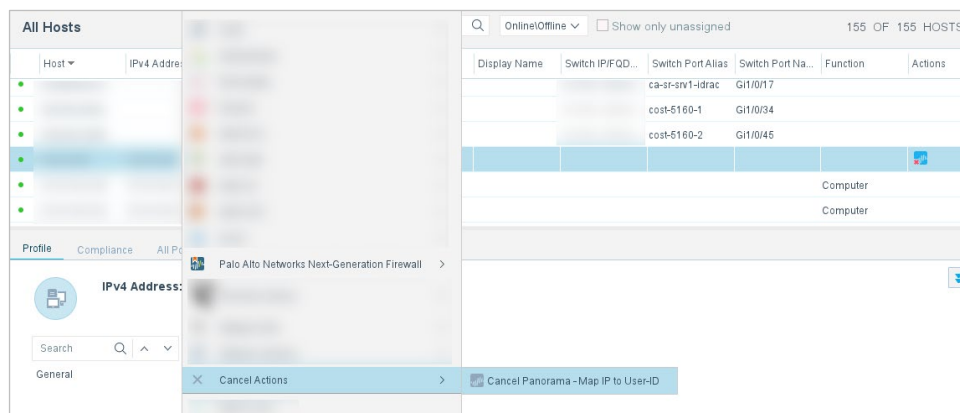
Cancel Panorama – Map IP to User-ID

Cancel the Panorama – Map IP to User-ID action.

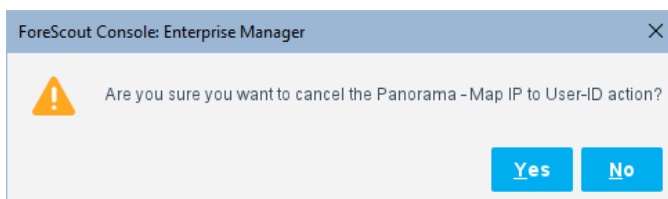
To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Panorama – Map IP to User-ID action configured.

2. Right click, select **Cancel Actions**, and then select **Cancel Panorama – Map IP to User-ID**.



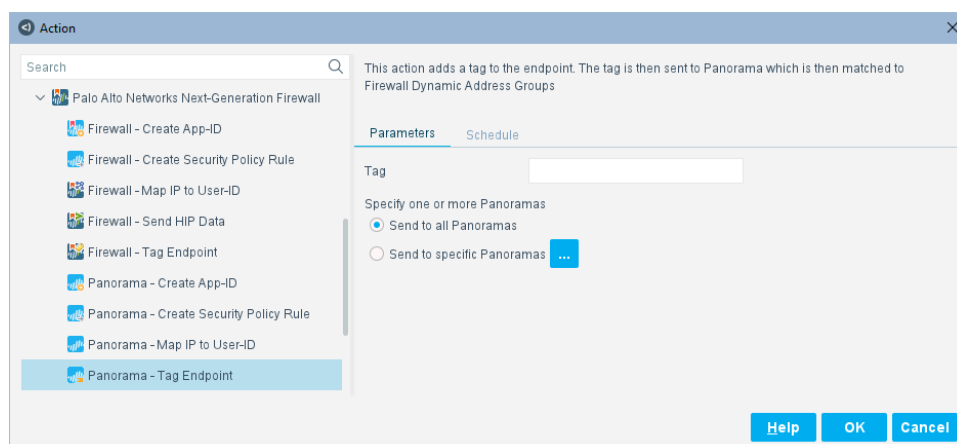
A confirmation is displayed.



3. Select **Yes**.

Panorama – Tag Endpoint

This action adds a tag to an endpoint, sends the tag to Panorama, which then matches the tag to Dynamic Address Groups.



The following parameters are available:

Tag	Enter a tag defined on the Panorama server in the Palo Alto Networks Next-Generation Firewall. Names are case sensitive.
------------	--

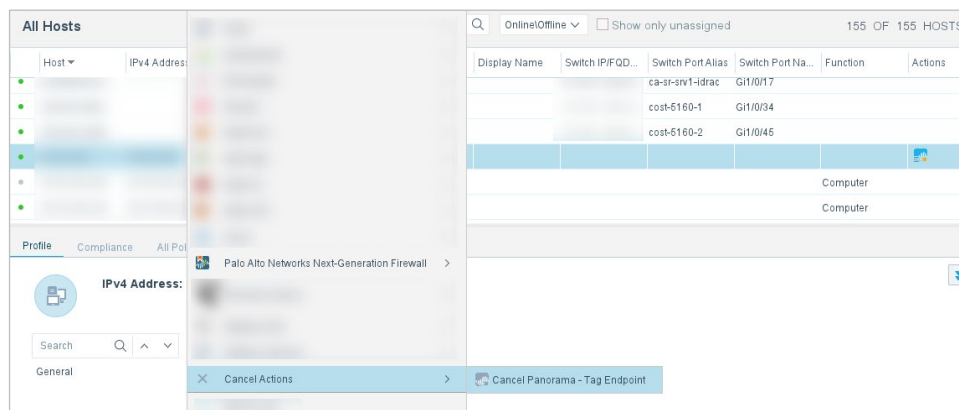
Specify one or more Panoramas	Specify one or more Panoramas: <ul style="list-style-type: none"> ▪ Send to all Panoramas: The action is applied to all Panorama servers. ▪ Send to specific Panoramas: The action is applied to selected Panorama(s). Select one or more Panorama(s) from the list of target Panorama servers.
--------------------------------------	---

Cancel Panorama – Tag Endpoint

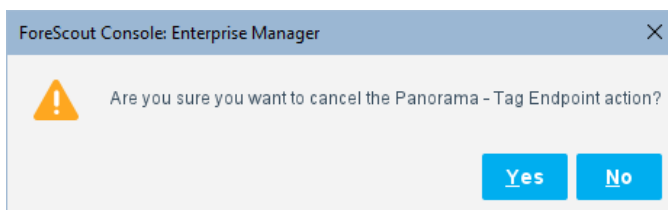
Cancel the Panorama – Tag Endpoint action.

To cancel the action:

1. In the **All Hosts** pane, select an endpoint with the Panorama – Tag Endpoint action configured.
2. Right click, select **Cancel Actions**, and then select **Cancel Panorama – Tag Endpoint**.



A confirmation is displayed.



3. Select **Yes**.

Work with Palo Alto Networks NGFW

This section covers the general use of Forescout eyeExtend for Palo Alto Networks NGFW.

Best Practices

- Once Forescout eyeExtend for Palo Alto NGFW is configured, the Forescout platform can include actions in policies affecting endpoints. In each case, administrators can define whether to send information to all Palo Alto firewalls or a set of specific firewalls in regional deployments.
- Sending User-ID information uses the standard format associated with Microsoft Active Directory (DOMAIN\username) to pass User-ID information to the Palo Alto Networks firewall. This is particularly important in environments where the Palo Alto Global Connect client is absent or is not fully deployed on all endpoints, so that firewall policies based on User-ID can remain effective in providing segmentation of traffic based on user groups.
- Where Palo Alto Networks segments or controls traffic based upon endpoint compliance status, the Forescout platform can provide timely information on compliance status by sending HIP data. HIP data can include data on running processes, encryption status, patch compliance, and antivirus status. This is particularly important in environments subject to regulatory requirements that require non-compliant endpoints to be blocked from connecting to resources where sensitive personal, financial, or health information is stored.
- For the Forescout platform to get the most out of the Firewall – Tag Endpoint action, tags need to be first defined on the Palo Alto NGFW. These tags include operators for determining which endpoints should be considered. The Forescout platform then takes those criteria and applies the tags appropriately across the enterprise.

A maximum of 32 tags are supported by Palo Alto NGFW. In general, most customers use 3 or less.

General Guidance

- Consider mapping CounterACT Appliances to Palo Alto Networks firewalls. If both these types of devices are deployed in a regional fashion, CounterACT Appliances in a particular region can be used as focal appliances for communication with the Palo Alto Networks firewalls in the region.
- Conversely, if the CounterACT Appliances are centrally deployed and Palo Alto Networks firewalls are in a distributed deployment, consider expediting the flow of information from the Forescout platform in general to the Palo Alto Networks NGFW deployment. To do this, utilize a specific firewall for communication within that same firewall. For example, if a Palo Alto Networks firewall controls access to the data center for servicing systems in Region A, then a Forescout platform responsible for endpoints in Region A would be best suited to communicate with that firewall. A Forescout platform responsible for endpoints in Region B would not be optimal.

- Resiliency for CounterACT Appliances responsible for communication with Panorama and Palo Alto Networks NGFWs is provided via High Availability. Cluster groups do not transfer communication responsibilities from one Forescout platform to another. This is because each appliance uses its own keys for communication with Panorama and Palo Alto Networks NGFWs; these keys are non-transferable.


Access the Asset Inventory

Once Forescout eyeExtend for Palo Alto Networks NGFW has been configured, you can view and manage the devices from Asset Inventory view in the Console. This provides activity information, accurate at the time of the poll, on endpoints based on specific instances' properties. The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View endpoints that are detected with specific attributes
- Incorporate inventory detections into policies

To access the inventory:

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **Palo Alto Networks Next Generation Firewall** folder.

 *If you did not configure the module to display the property in the Asset Inventory, your Palo Alto Networks NGFW properties are not displayed in the Views pane of the Asset Inventory.*

3. Check that the properties match the configuration requirements.

Access the Home Tab

To access the Home tab:

1. In the Console, select **Home**.
2. In the Views tree, expand **Policies** and then select **Palo Alto Networks Next-Generation Firewall**.
3. Select an item in the Detections pane. The Profile, Compliance, and All Policies tabs display the information related to the selected host.

Refer to *Working on the Console > Working with Inventory Detections* in the *Forescout Administration Guide* or the Console Online Help for information about working with the Asset Inventory. See [Additional Forescout Documentation](#) for information on how to access this guide.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.