FORESCOUT

Forescout

eyeExtend for Palo Alto Networks Next-Generation Firewall

Configuration Guide

Version 1.3

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

Legal Notice

2019-03-12 13:55

Table of Contents

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, and 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.*

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.

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***

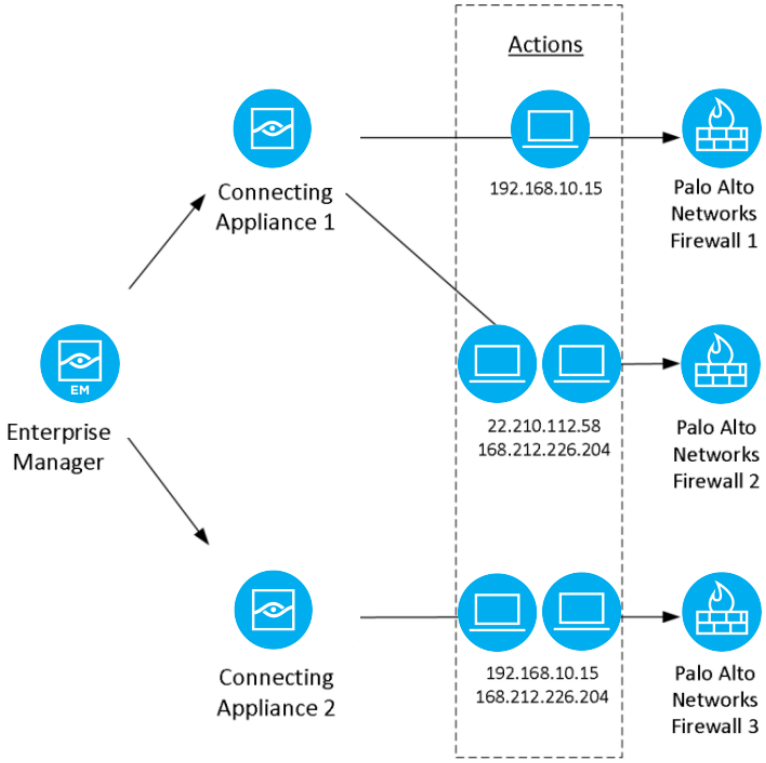
  You can leverage Palo Alto's use of tags as filtering criteria to determine the members of dynamic address groups. Using tags, the Forescout platform can dynamically add endpoints to dynamic address groups based on endpoint assessment in policies. See Tag Endpoint.

- ***Leverage the Forescout platform as a mission-critical real-time information source***

  - ***Map endpoint IP addresses discovered by the Forescout platform to firewall 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 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 Send HIP Data.

How It Works

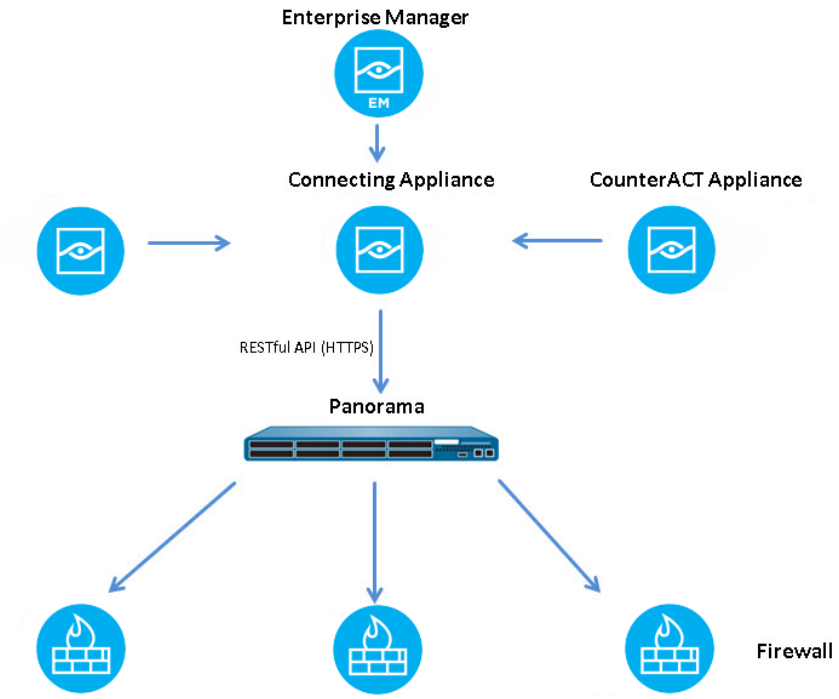
In addition to working directly with each firewall, Forescout eyeExtend for Palo Alto Networks NGFW integrates with the Palo Alto Network's central management system, Panorama, which manages a distributed network of virtual or physical firewalls.



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 using the Forescout Map IP to User-ID, Send HIP Data, and Tag Endpoint 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 Map IP to User-ID, Send HIP Data and Tag Endpoint actions. See Palo Alto Networks Next-Generation Firewall 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 8.1.
- Content Module with the Windows Applications Plugin component running.
- Endpoint Module version 1.1, 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.

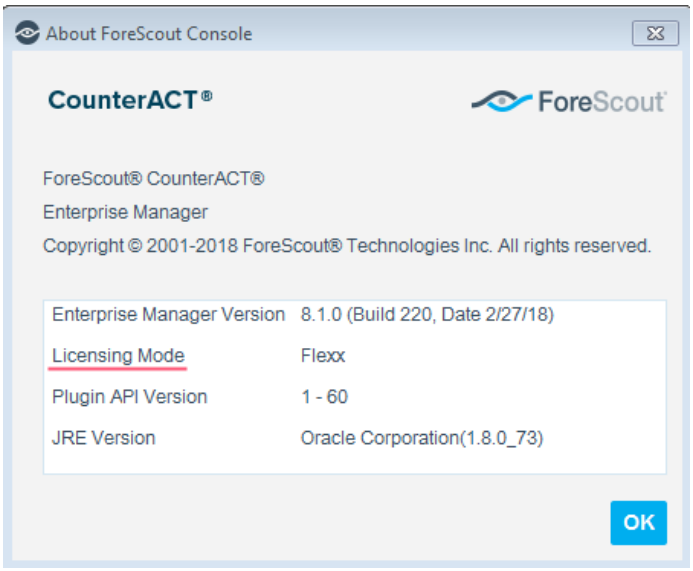
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend product 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.

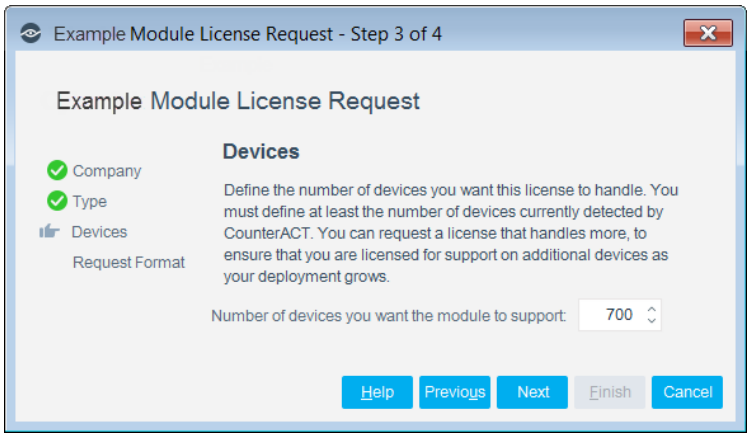
Demo license extension requests and permanent license requests are made from the Console.

> *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 products. 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 products. 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 products, packaging individual licensed modules are supported. T*he Open Integration Module is an *eyeExtend* product 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

This module requires Palo Alto Networks Firewall running one of the following versions of PAN-OS:

- 6.0.x
- 6.1.x

- 7.0.x
- 7.1.x
- 8.0.x
- 8.1x

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 will not proceed if you do not agree to the license agreement.

   The installation will begin 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 generating an API key for information about API key management in the *PAN-OS Administrator's Guide*. This information is also available on the following website:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/70/pan-os/pan-os.pdf

Prepare Your Security Policy – Create a Dynamic Address Group

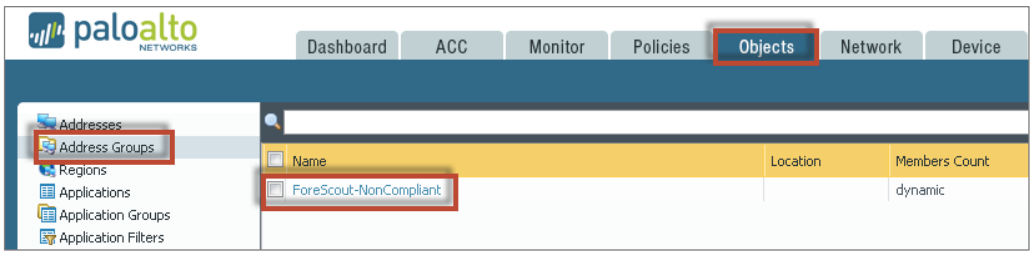
Dynamic Address Groups let you create a Forescout platform policy that automatically adapts to changes based on the filtering criteria of tags. These changes include additions, moves, or deletions of servers. It also provides flexibility for applying different rules to the same server based on its role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

To configure a Dynamic Address Group:

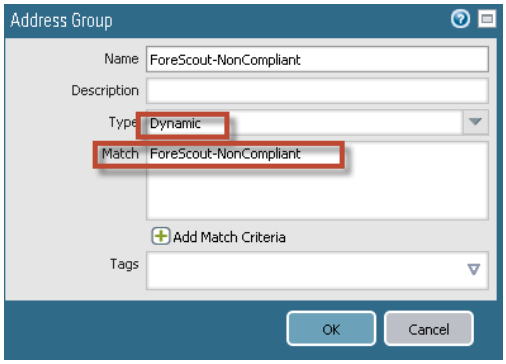
1. Log in to the web interface of the firewall.

   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**.



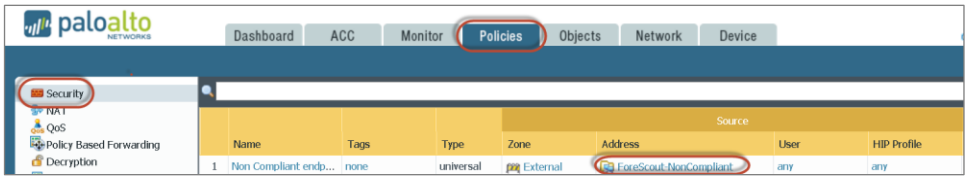
3. Select **Add**.



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 tags. See Define the Panorama Server.
- Define each firewall server and its login credentials, and import the tags. See Define 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.

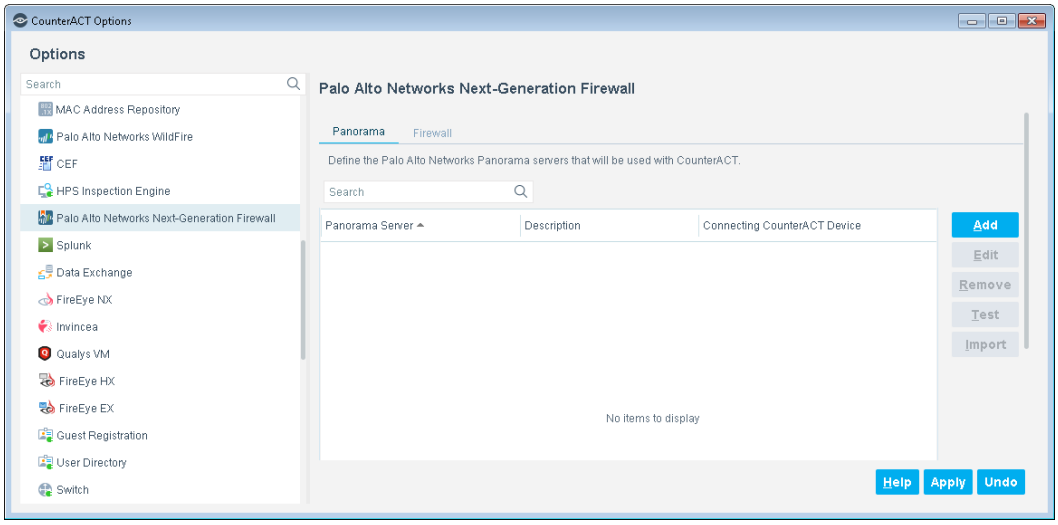
Before configuring the module, review the How It Works section.

Define the Panorama Server

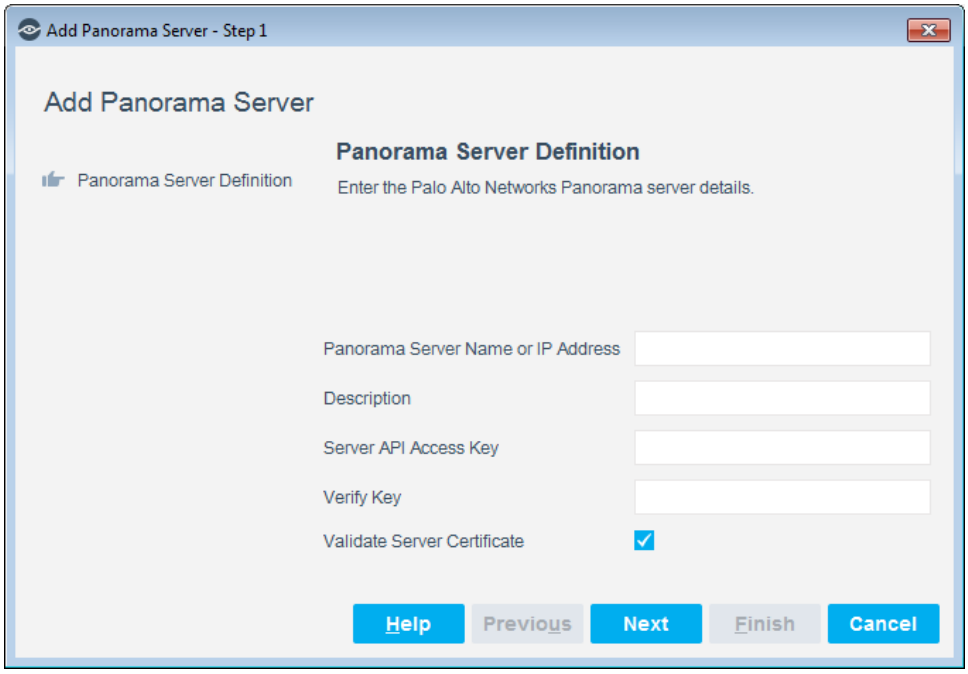
Configure the Panorama server details and Connecting CounterACT device.

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	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product 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*.

*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, select **Import** in the Palo Alto Networks Next-Generation Firewall pane.*

6. Select **Next**.

7. Configure the Connecting CounterACT device:

Connecting CounterACT Device	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	▪ **SSL** – Select the preferred secured communication version to use. ▪ **TLS v 1.2** – 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.

8. Select **Finish**. The new server is listed in the Palo Alto Networks Next-Generation Firewall pane.
9. If you have PAN firewalls that are managed by Panorama servers, select **Import**.

You need to perform Import every time a new server is added to the Panorama Server and you want to add it to the module.

10. Select **Apply**.

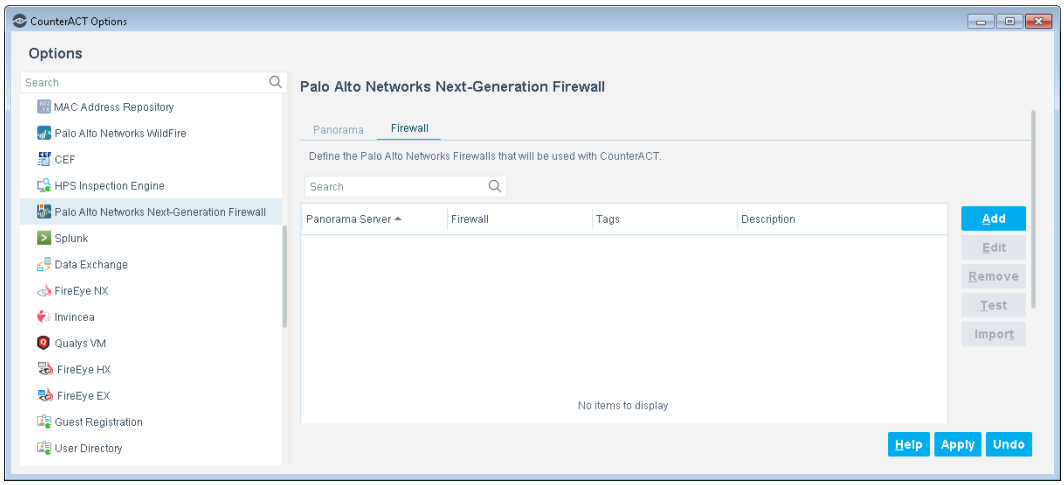
The best practice is to perform a test after setting up a connection. See Test the Module Configuration.

Define Individual Firewalls in the Forescout Platform

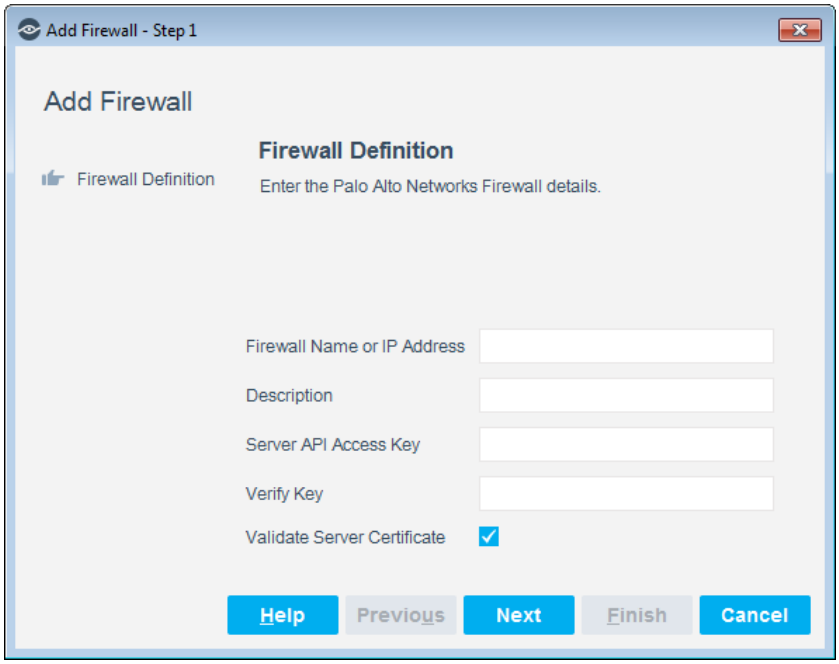
Configure individual firewall options to determine when API calls are sent from Forescout eyeExtend for Palo Alto Networks NGFW to the firewall.

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.



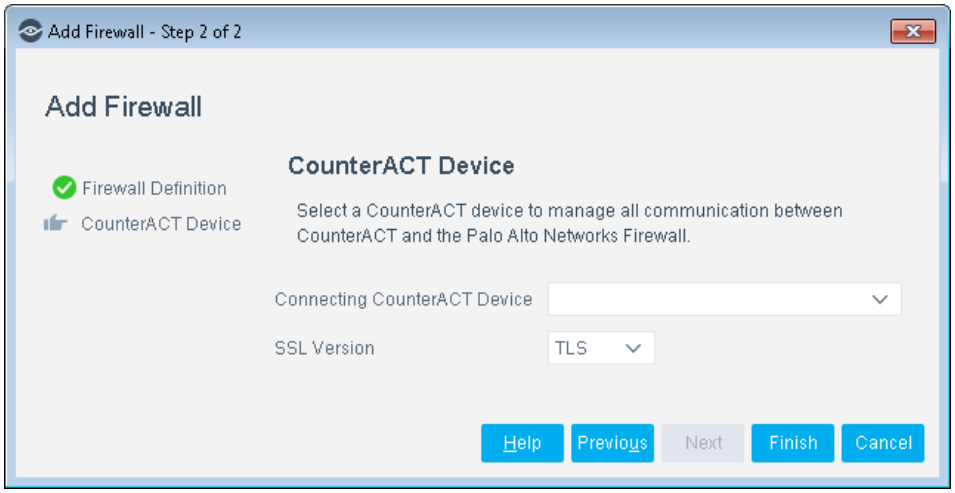
3. Select **Add**.



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.
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.
Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product 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**.



6. Select 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	▪ **SSL** – Select the preferred secured communication version to use. ▪ **TLS v 1.2** – 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 in the Palo Alto Networks Next-Generation Firewall pane.
8. Select **Apply**.

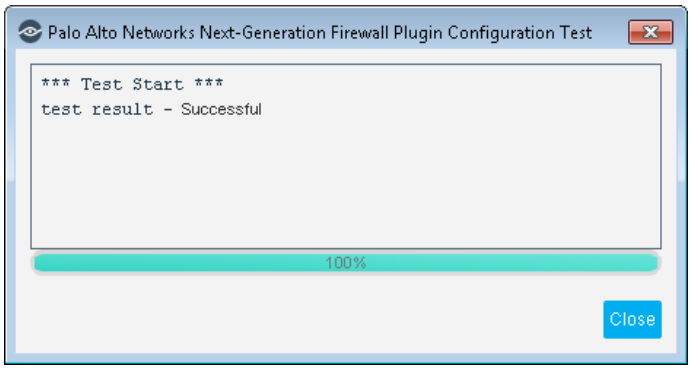
The best practice is to perform a test after setting up a connection. See Test the Module Configuration.

Test the Module Configuration

This section describes how to perform a configuration test. This 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.

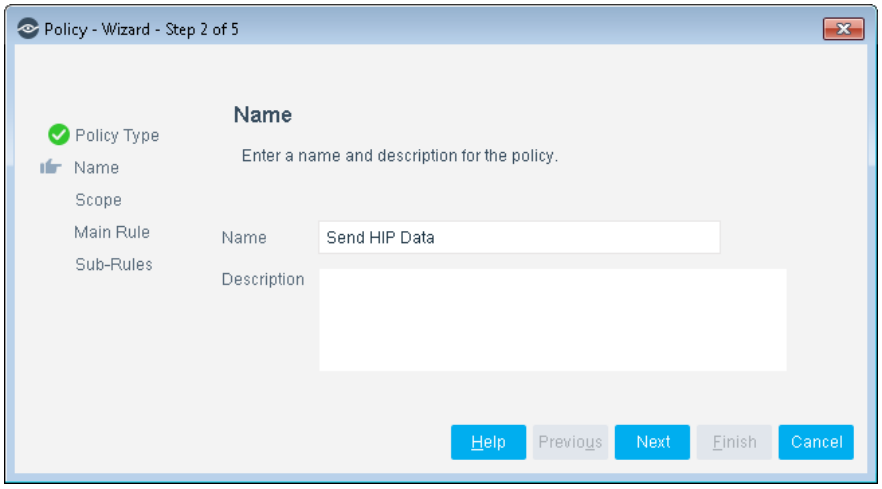
Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

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. The Policy Wizard opens.

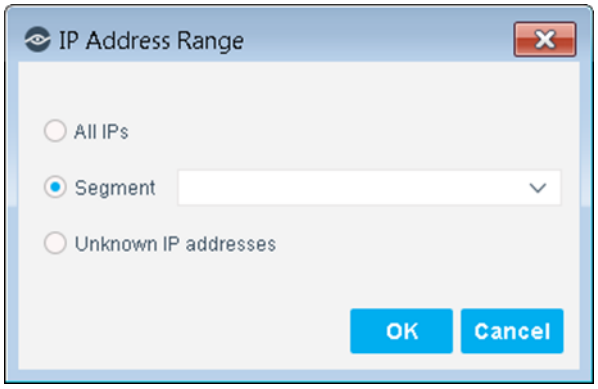
3. Expand the **Palo Alto Networks Next-Generation Firewall** folder and select **Send HIP Data**. The Send HIP Data pane opens.
4. Select **Next**.



5. Define a unique name for the policy you are creating based on this template, 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.



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.
9. Select **Next**. The Main Rule pane opens.
10. Select **Next**. The Sub-Rules pane opens.
11. Select **Finish** to create the policy.
12. In the Policy Manager, select **Apply** to save the policy.

How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. 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.

Main Rule

The main rule of this policy applies a filter to Windows, Linux or Mac manageable devices.

Sub-Rules

A policy sub-rule has been 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 PAN firewall, such as user, domain, OS, AV enable status, and patch enable status. The action then sends whatever property is available to the PAN firewall. The sub-rules for Linux and Mac are set up in a similar way.

By default, these actions are disabled.

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 Next-Generation Firewall 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 Module actions:

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

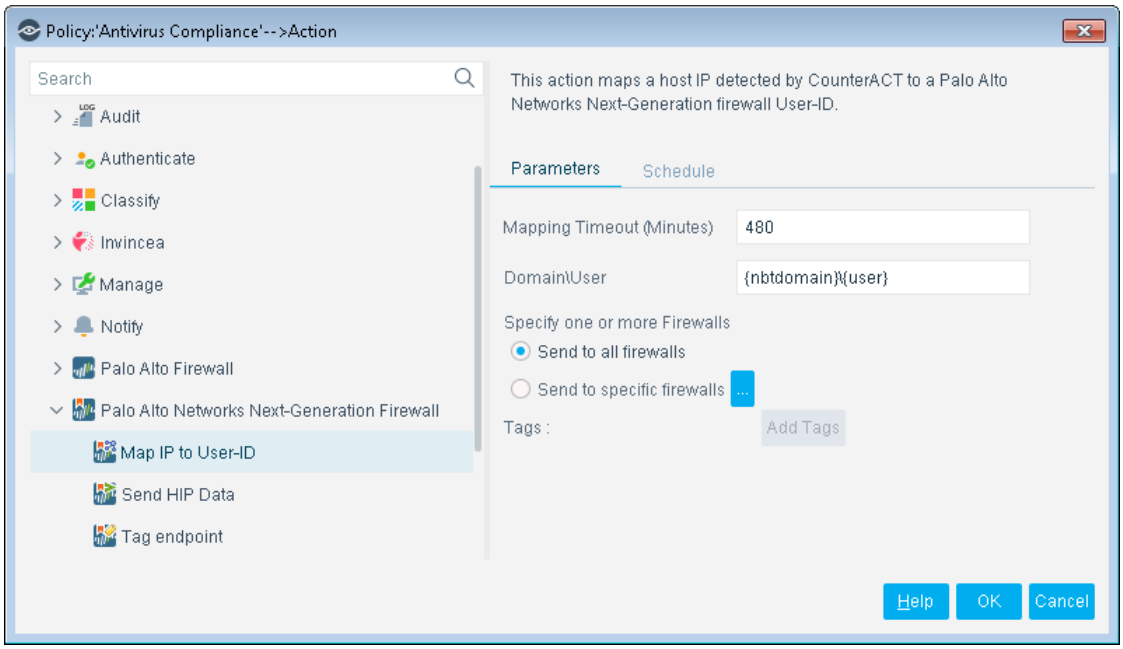
  The following actions are available:

  - Map IP to User-ID
  - Send HIP Data
  - Tag Endpoint

Map IP to User-ID

This action lets you map an endpoint IP address detected by the Forescout platform to a Palo Alto Networks NGFW 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)	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 *nbtdomain* and *user* property tags representing the NetBIOS domain and the user name. You can select any property tag by using the Tags option.
Specify one or more Firewall Servers	The target firewall(s) that the action is applied to. See Configure the Module.

Send HIP Data

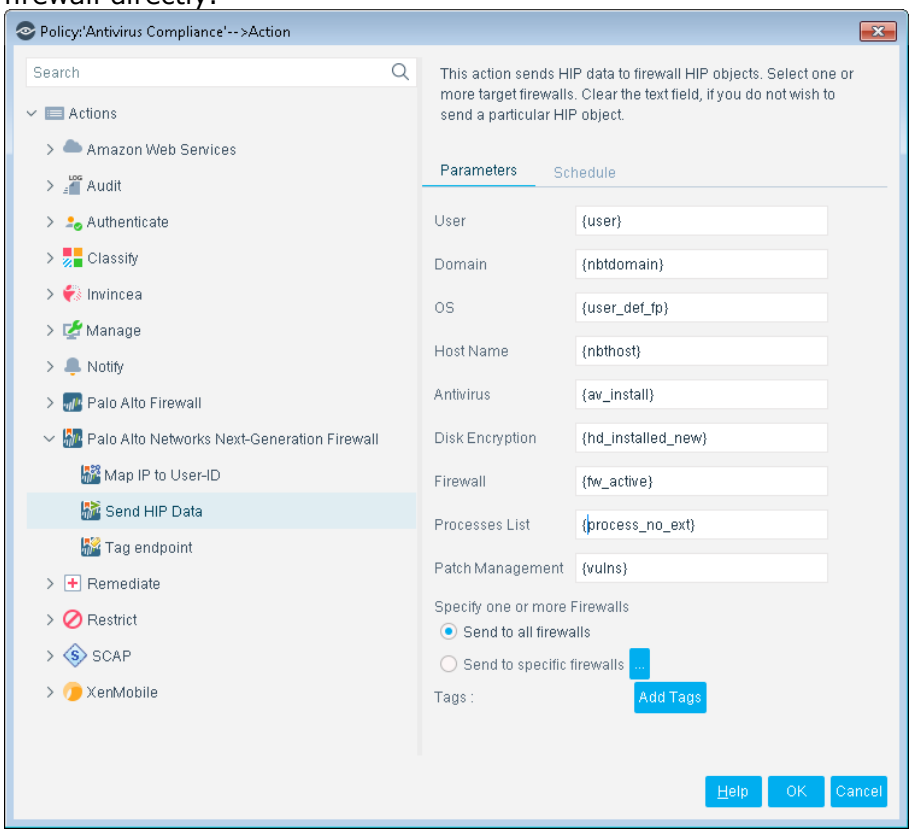
This action lets you send endpoint host properties that correspond to HIP data fields to the PAN firewall, where the information can be used to further filter access and create a more restrictive policy. This enables better security control.

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

The Forescout platform can send HIP information to Panorama or to the firewall directly.



PAN 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
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_process_running}`	Mac/Linux property scanner

Parameter	OS	Data Sent	Default Forescout Platform Property	Dependency
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:

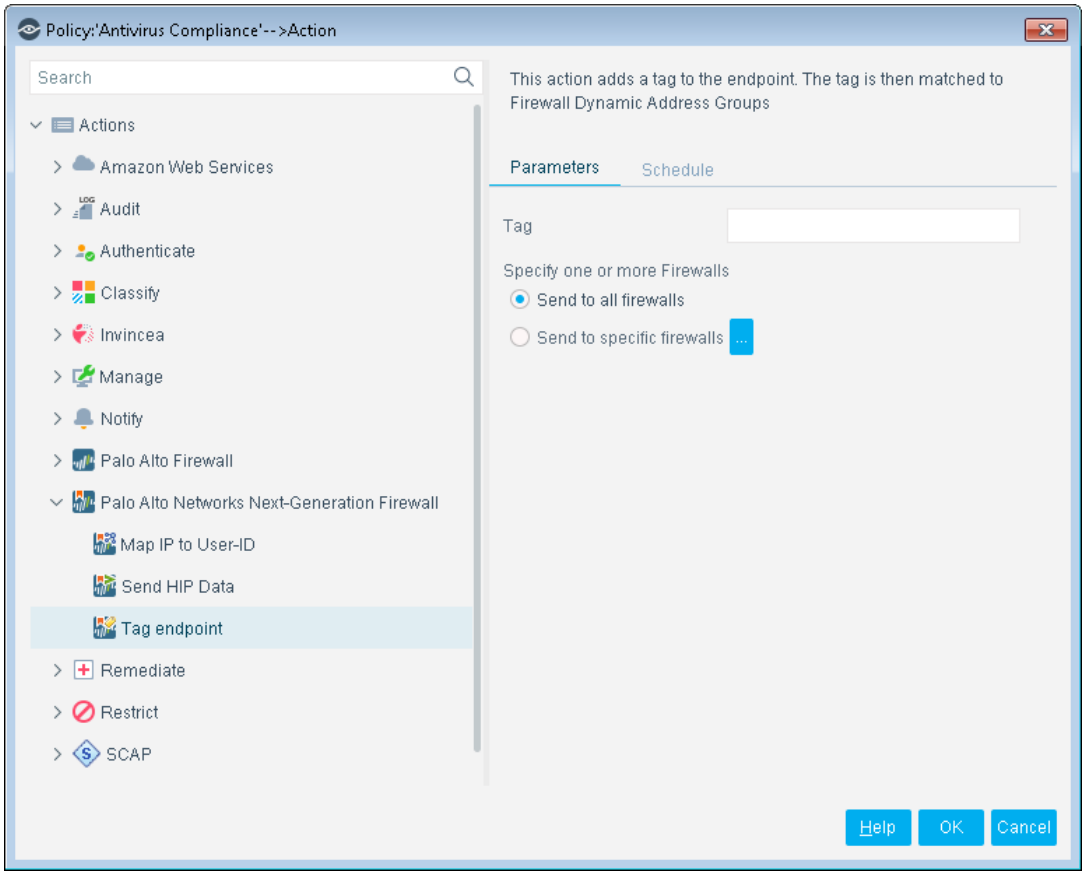
Send to all firewalls	Sends HIP data to all firewall servers.
Send to specific firewalls	Sends HIP data to selected firewalls only. Select one or more firewalls from the list of target firewall servers.

Tag Endpoints

This action adds a tag to an endpoint. The tag is then matched to a Firewall Dynamic Address Group by the PAN 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.
All Firewall Servers	The action is applied to all firewall servers.
Specify servers	The action is applied to selected firewalls. Select one or more firewalls from the list of target firewall servers.

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 the actions of Map IP to User-ID, Send HIP Data, and Tag endpoint 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 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 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 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 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 firewalls in the region.
- Conversely, if the CounterACT Appliances are centrally deployed and Palo Alto firewalls are in a distributed deployment, consider expediting the flow of information from the Forescout platform in general to the Palo Alto NGFW deployment. To do this, utilize a specific firewall for communication within that same firewall. For example, if a Palo Alto 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 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 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.

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 Forescout Resources Page, or 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 Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of 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 Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer 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.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information 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.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

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

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).