ForeScout® Extended Module for Palo Alto Networks® Next Generation Firewall

Configuration Guide

Version 1.2

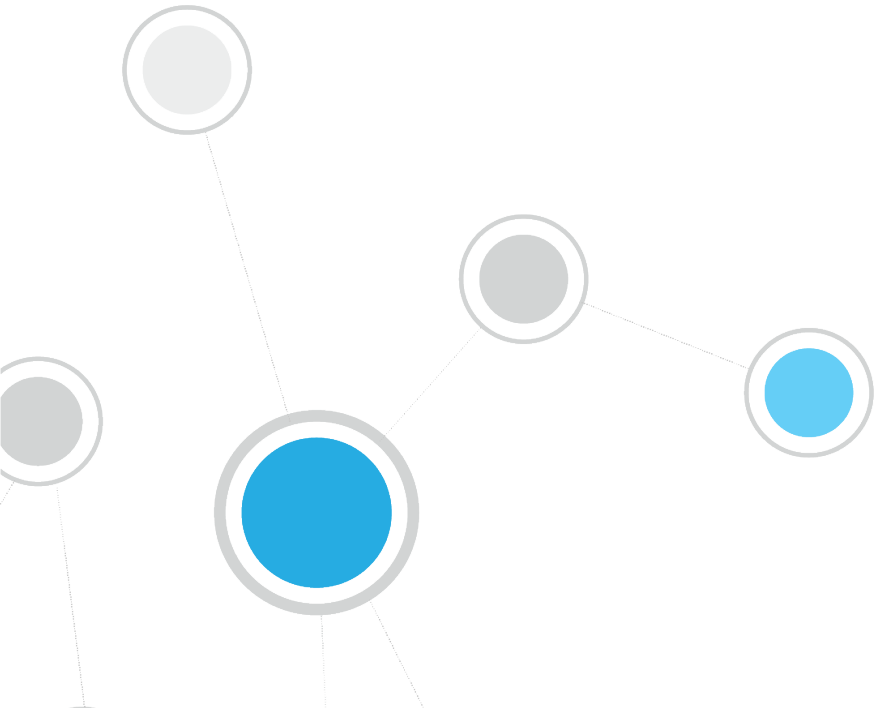


Table of Contents

About the Palo Alto Networks Next-Generation Firewall Integration

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

The integration allows security teams to:

- 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 CounterACT policies and other basic features work.

Use Cases

This section describes use cases supported by this module. Be sure to review the Best Practices.

To understand how this module helps you achieve these goals, see About the Palo Alto Networks Next-Generation Firewall Extended Module.

Roll-out Dynamic Firewall Access Control Powered by CounterACT Policy Detections

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

Dynamic Firewall Access Control Powered by CounterACT Policy Detections

Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, OS, location, risk status and more. This information is learned by CounterACT 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 CounterACT, otherwise unavailable without the Palo Alto Networks GlobalProtect Agent installed on network endpoints.

Relying on CounterACT 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 CounterACT detected IPs to user IDs to support granular filtering of users rather than IP addresses. CounterACT-based IP to User-ID capabilities provide vital support in environments where Active Directory is not available or limited.

About the Palo Alto Networks Next-Generation Firewall Extended Module

The Palo Alto Networks Next-Generation Firewall Module lets you integrate CounterACT 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 CounterACT can dynamically add endpoints to dynamic address groups based on endpoint assessment in policies. See Tag Endpoint.

- ***Leverage CounterACT as a Mission-critical Real-time Information Source***

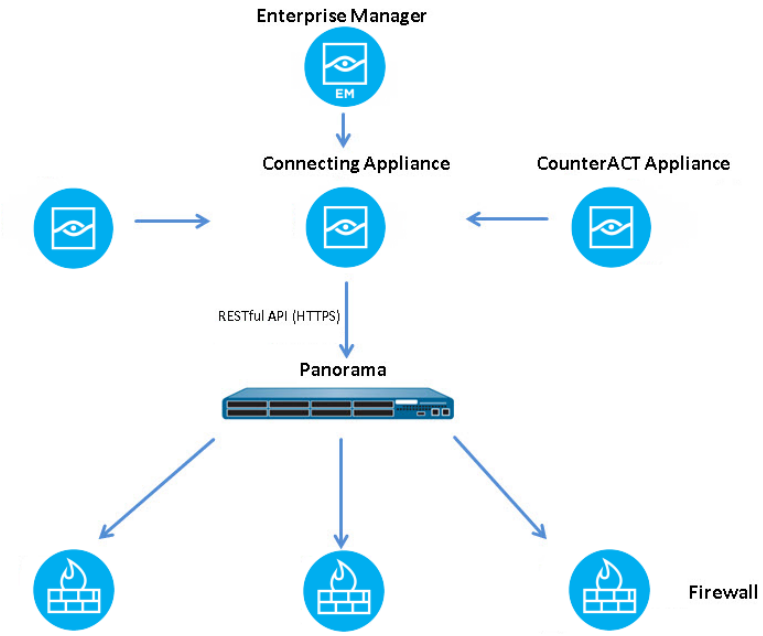
  - ***Map endpoint IP addresses discovered by CounterACT to firewall User-IDs***. For example, the module can map the IP address of a user authenticating to a captive portal through a proxy. See Map IP to User-ID.
  - ***Send HIP (Host Information Profiles) data***. Use endpoint properties such as domain name and operating system discovered by CounterACT for policy enforcement. See Send HIP Data.

How it Works

This section describes how the module communicates with Palo Alto Networks Panorama Server and firewalls.

Central Firewall Management

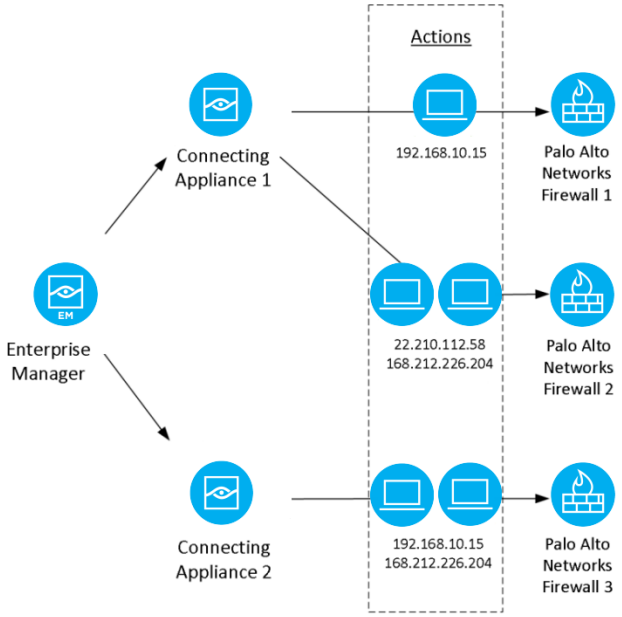
In addition to working directly with each firewall, the module integrates with the Palo Alto Network's central management system, Panorama, which manages a distributed network of virtual or physical firewalls.



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

The module communicates with Palo Alto Networks firewalls, supplying endpoint IP address information discovered by CounterACT using the CounterACT *Map IP to User-ID*, *Send HIP Data* and *Tag Endpoint* actions.

Each firewall is assigned to a 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.



What to Do

You must perform the following to work with this module:

1. Verify that 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 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

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- Palo Alto Networks Next-Generation Firewall Requirements

CounterACT Software Requirements

The module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- Content Module version 1.0 with the Windows Applications Plugin component running.
- Endpoint Module version 1.0 with the following components running:
  - HPS Inspection Engine
  - Linux
  - OS X
- This module is a component of the Palo Alto Networks Next-Generation Firewall Extended Module and requires a module license. See ForeScout Module License Requirements for details.
- An active Maintenance Contract for the module.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this component.*** The functionality described in this document is

based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

ForeScout Extended Module License Requirements

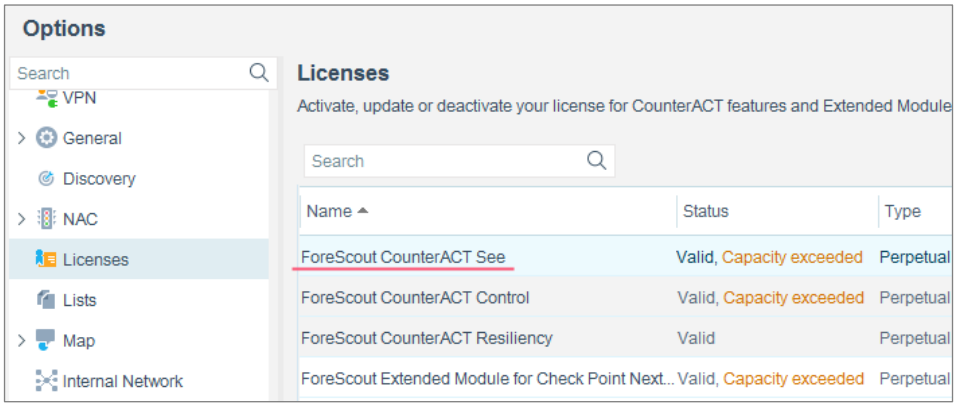
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

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

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

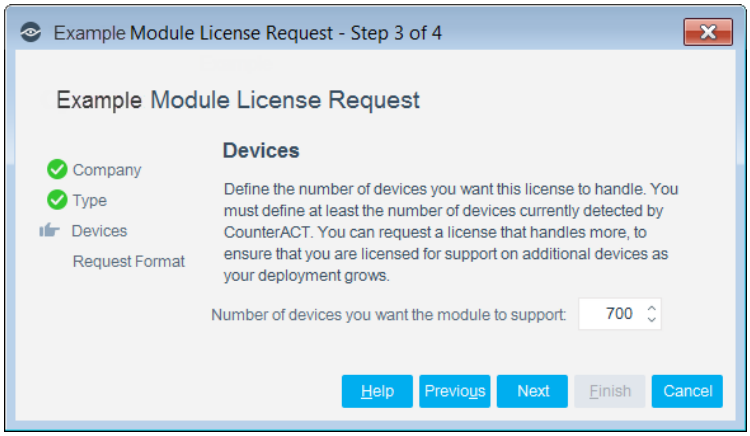
Demo license extension requests and permanent license requests are made from the CounterACT Console.

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 CounterACT 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 CounterACT. 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 CounterACT, 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.

Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint

capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

- *Integration Modules, which package together groups of related licensed modules, are not supported when operating in Centralized Licensing Mode. Only Extended Modules, packaging individual licensed modules are supported. T*he Open Integration Module is an Extended Module even though it packages more than one module.

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

Palo Alto Networks Next-Generation Firewall Requirements

The 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

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 - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.

2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT 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.

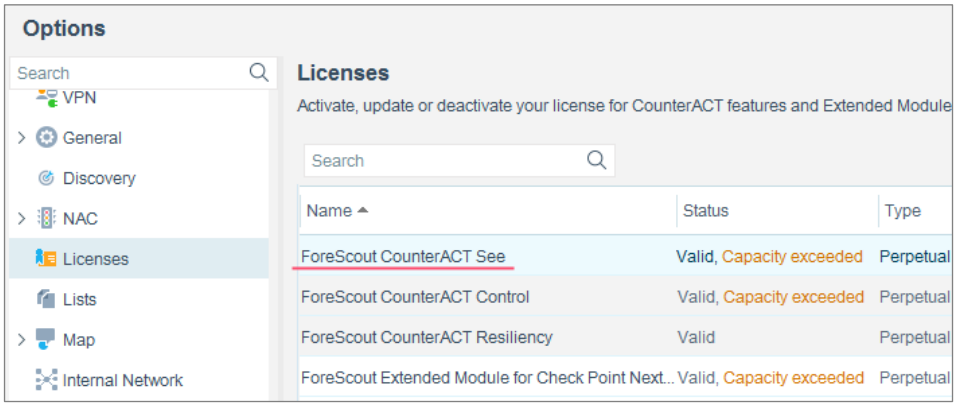
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

Some components are not automatically started following installation.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Palo Alto Networks Next-Generation Firewall Set Up

This section describes how to:

- Generate an API Key
- Prepare Your Security Policy - Create a Dynamic Address Group

Generate an API Key

To access the Server API, CounterACT 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*. Here you will also find information about API key management. This information is also available at

https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/device-management/use-the-xml-api

Prepare Your Security Policy - Create a Dynamic Address Group

This section describes how to configure a Dynamic Address Group on the firewall.

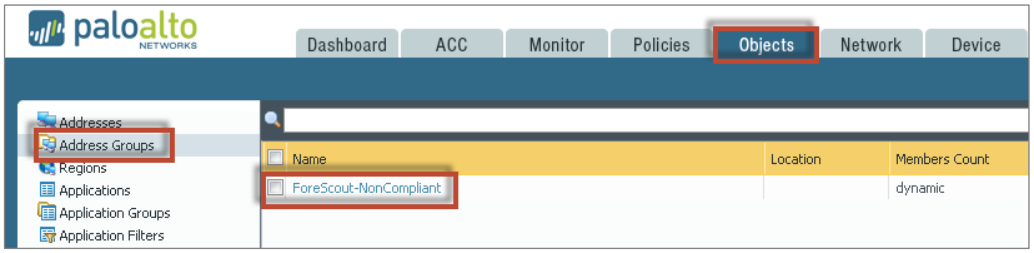
Dynamic Address Groups allow you to create a CounterACT policy that automatically adapts to changes based on the filtering criteria of tags. These changes include additions, moves, or deletions of servers. It also provides flexibility for applying different rules to the same server based on its role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

To configure a Dynamic Address Group:

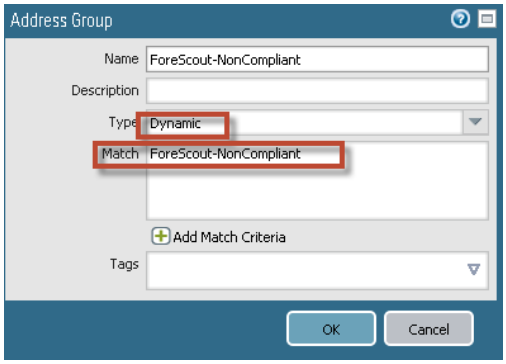
1. Log in to the web interface of the firewall.

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** and give the Dynamic Address Group a name. Under **Type**, select **Dynamic**.

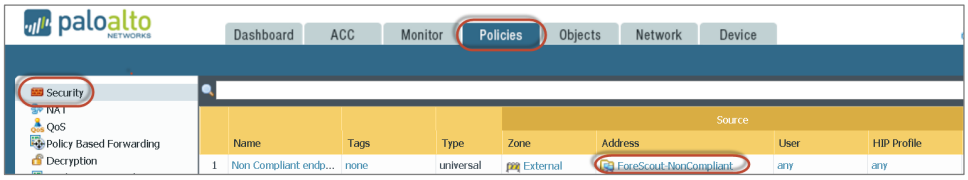


4. Select **Add Match Criteria**. Since the tags are registered dynamically, add the Match Criteria to the Dynamic Group **Match** field.

   The Match Criteria you define will be available for selection in the CounterACT Action.

5. Select **OK** and then **Commit**.

6. Use the group in the firewall policy based on your security requirements



Configure the Module

Configure the module for CounterACT to communicate with the Palo Alto Networks service.

- Define the Panorama server, including the name of the defined Panorama server and the CounterACT device it communicates with and import the firewalls and tags. See Configure the Panorama Server.
- Define each firewall server and its login credentials and import the tags. 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 CounterACT, 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.

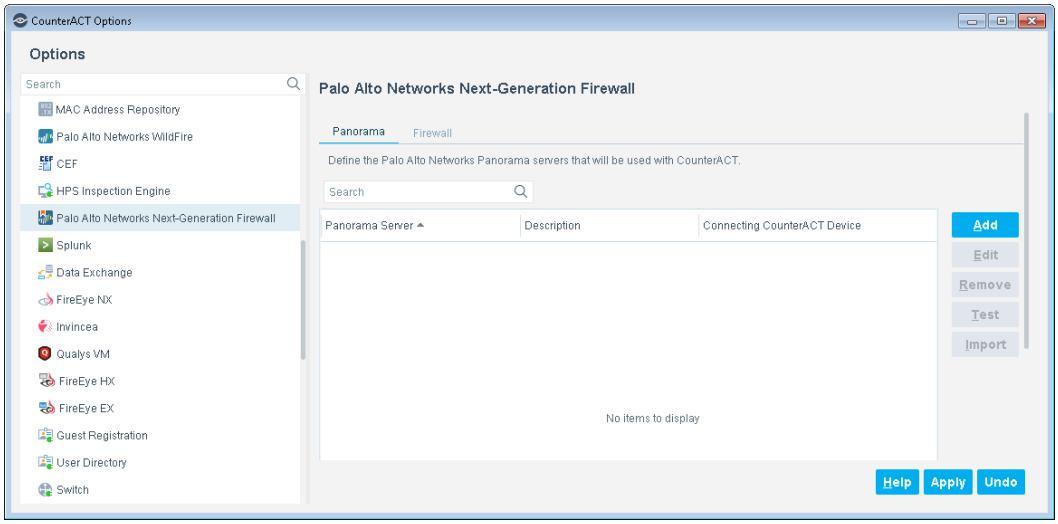
Before configuring the module, review the How it Works section.

Configure the Panorama Server

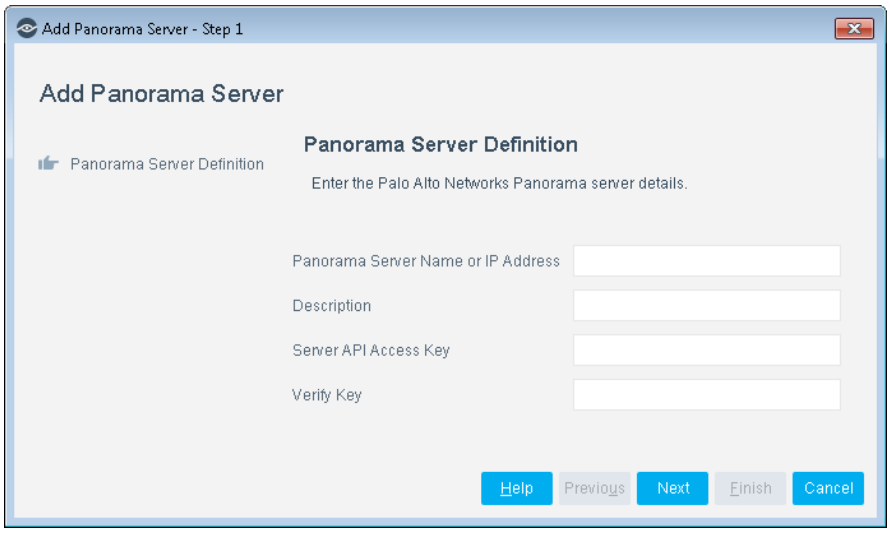
Configure the Panorama server details and Connecting CounterACT device.

To configure the Panorama Server:

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



3. In the right pane, ensure that the **Panorama** tab is selected.
4. Select **Add**. The Add Panorama Server dialog box opens.



5. In the **Panorama Server Definition** pane, configure the following connection parameters:

Panorama Server Name or IP Address	Resolvable DNS name or IP address.
Description	Internal description of Panorama in CounterACT.
Server API Access Key	Acquired for API authentication.
Verify Key	Re-enter key.

6. Select **Next**. The **CounterACT Device** pane opens.

7. Set the configurations for the Connecting CounterACT device.

Connecting CounterACT Device	The IP address of the CounterACT device that communicates with the firewall server. See 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 this selection in CounterACT is the same as what is configured on the Palo Alto Panorama server.*

8. Select **Finish**. The Palo Alto Networks Next-Generation Firewall pane displays with the new server listed.
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.

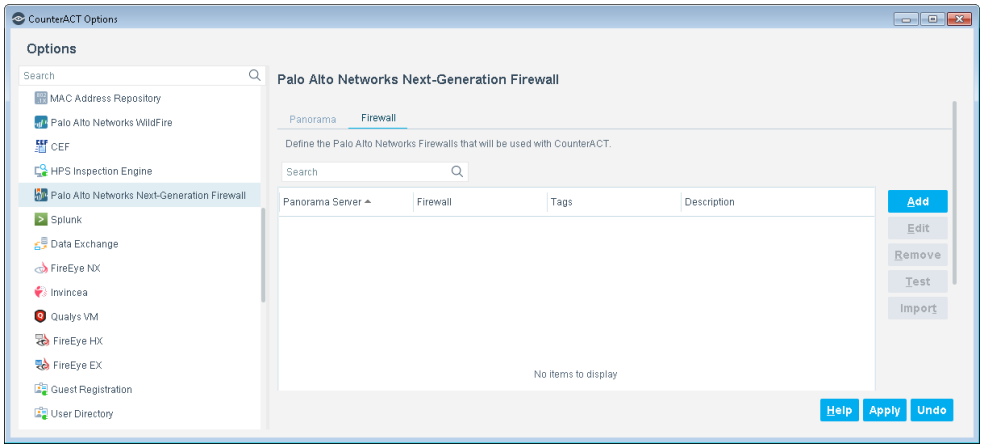
10. Select **Apply**.

Configure Individual Firewalls

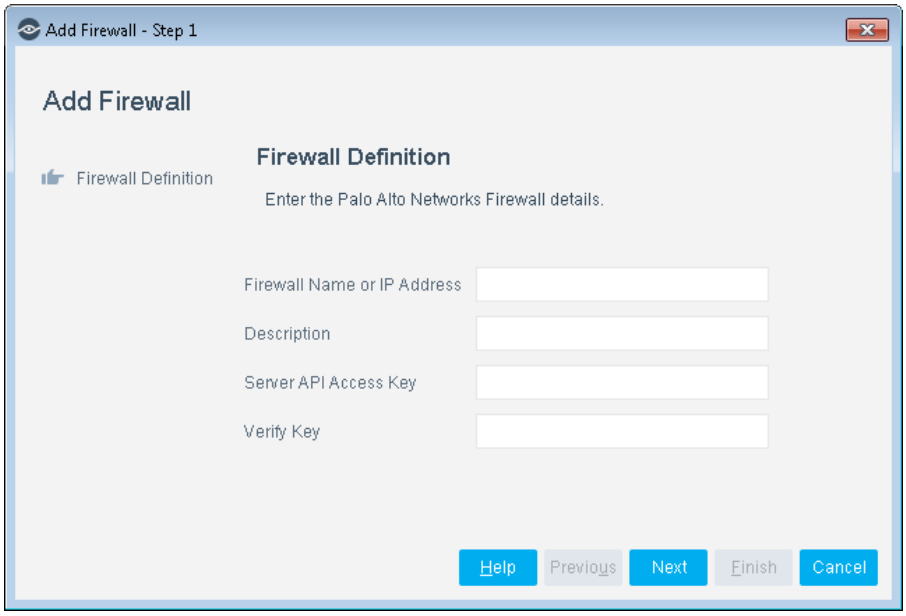
Configure individual firewall options to determine when API calls are sent from the module to the firewall.

To configure the firewall:

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



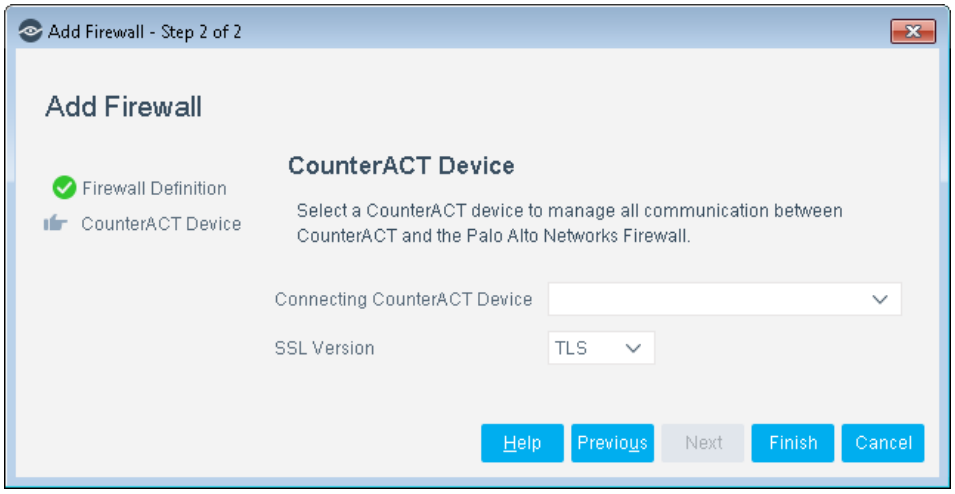
3. Select the **Firewall** tab.
4. Select **Add**. The Add Firewall dialog box opens.



5. In the **Firewall Definition** pane, configure the following connection parameters:

Firewall Name or IP Address	IP address or resolvable DNS name.
Description	Description of the Firewall name.
Server API Access Key	Acquired for API authentication.
Verify Key	Re-enter key.

6. Select **Next**. The **CounterACT Device** pane opens.



7. Select the **Connecting CounterACT Device**.

Connecting CounterACT Device	The IP address of the CounterACT device to communicate with the firewall server. See Palo Alto Networks Next-Generation Firewall Set Up 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 this selection in CounterACT is the same as what is configured on the Palo Alto Firewall.*

8. Select **Finish**. The Palo Alto Networks Next-Generation Firewall pane lists the new firewall.
9. Select **Apply**.

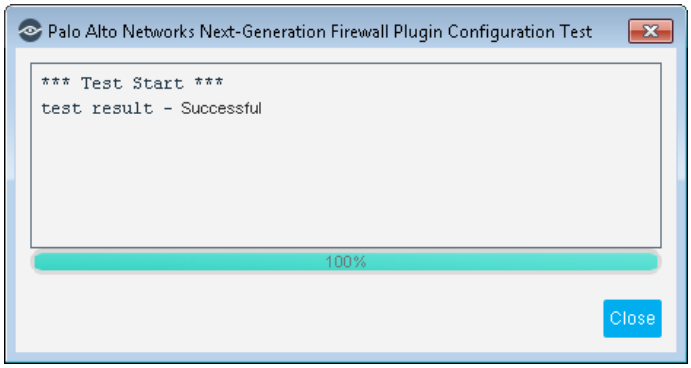
Test the Module Configuration

This section describes how to 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**.

   The Palo Alto Networks Next-Generation Firewall Module Configuration Test dialog box displays the test results.



3. Select **Close**.

Run Palo Alto Networks Next-Generation Firewall Policy Templates

CounterACT 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.

The following template is available for detecting and managing endpoints:

- Send HIP Data Policy Template

Send HIP Data Policy Template

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

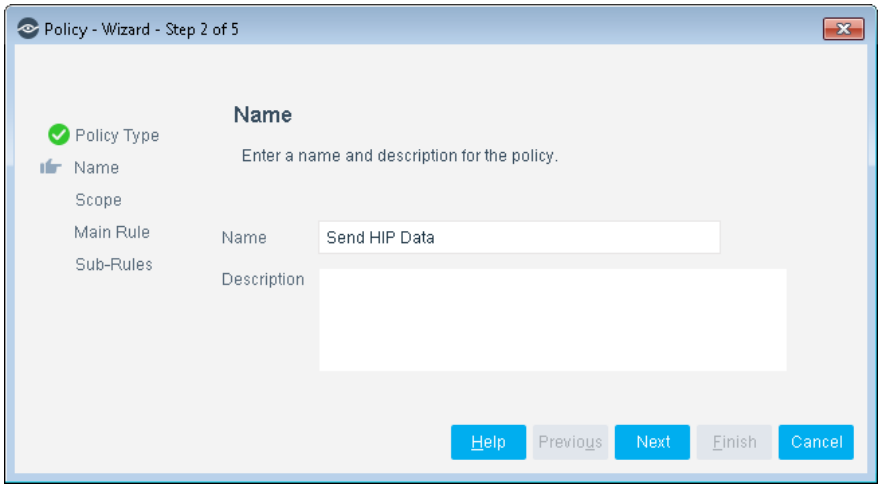
To use the Palo Alto Networks Next-Generation Firewall Send HIP Data Policy Template:

1. Log in to the CounterACT Console and select the **Policy** tab.
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**. The Name pane opens.

Name the Policy

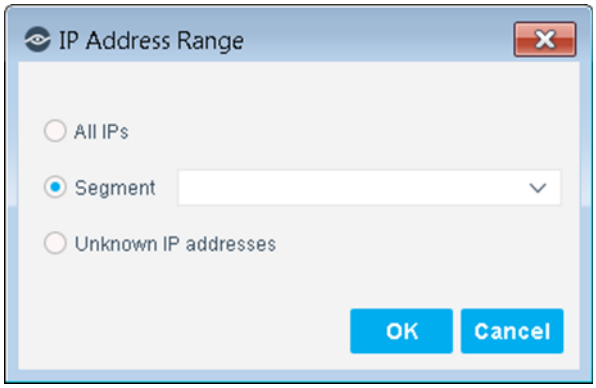
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



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.
6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

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 page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens.

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 CounterACT 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.

10. Select **Next**. The Sub-Rules pane opens.

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, patch enable status, etc. The action then sends whatever property is available to the PAN firewall. The sub-rules for Linux and Mac are similarly setup.

By default, these actions are disabled.

11. Select **Finish** to create the policy.
12. On the Policy Manager, select **Apply** to save the policy.

Create Custom Palo Alto Networks Next-Generation Firewall Policies

Use CounterACT policies to:

- Enhance firewall intelligence with dynamic, real-time information on endpoint compliance, functionality, OS, location, risk status and more. This information is learned by CounterACT policies and delivered to the firewall to deal with rapid network changes.
- Leverage CounterACT 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 CounterACT to apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

Actions

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

In addition to the bundled CounterACT actions available for detecting and handling endpoints, you can work with Palo Alto Networks Next-Generation Firewall module related 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 CounterACT Console.
2. Select the **Policy** icon from the Console toolbar.
3. Create or edit a policy.

Palo Alto Networks Next-Generation Firewall Policy Actions

This section describes the actions that are made available when the Palo Alto Networks Next-Generation Firewall module is installed.

To access Palo Alto Networks Next-Generation Firewall Module actions:

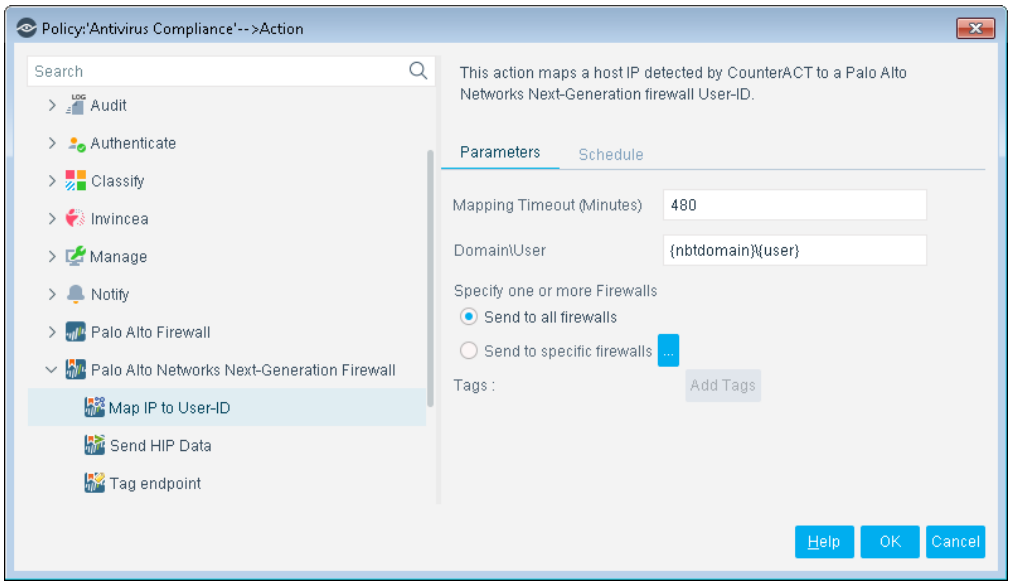
1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Palo Alto Networks Next-Generation Firewall folder in the Actions tree. The following actions are available:
   - Map IP to User-ID
   - Send HIP Data

- Tag Endpoint

Map IP to User-ID

This action lets you map an endpoint IP address detected by CounterACT to a Palo Alto Networks Next-Generation Firewall User-ID. CounterACT detects a fully qualified domain name (FQDN) to map an endpoint IP address.

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

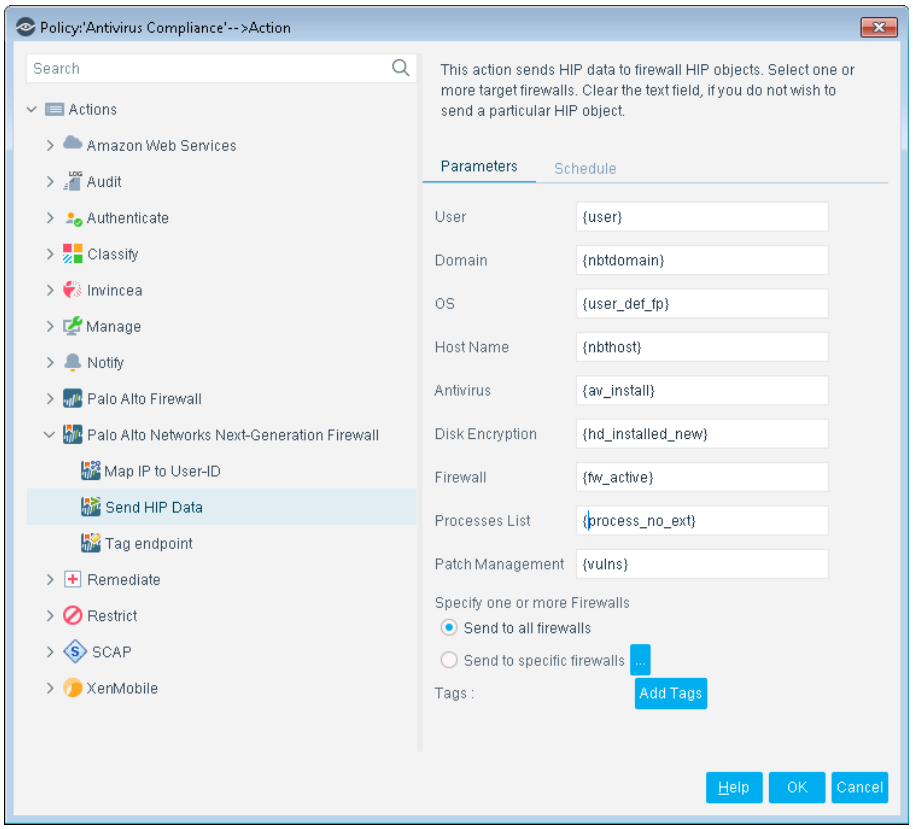
Send HIP Data

This action lets you send the following endpoint host properties, if available, to the PAN firewall where the information can be used to further filter access and create a more restrictive policy. This allows better security control.

CounterACT can populate the following information in the first version of the module on the PAN firewall:

- User, OS, Domain, 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

CounterACT can send HIP information to Panorama or to the firewall directly. Refer to the table below to see which PAN HIP object is mapped to a CouterACT host property and the module provides that host property.



The following parameters are available:

Parameter	OS	Data Sent	Default CounterACT Property	Dependency
User	Windows	Logged in User	**{user}**	HPS Inspection Engine
	Mac	Logged in User	**{mac_logged_users}**	Mac / Linux Property Scanner

Parameter	OS	Data Sent	Default CounterACT Property	Dependency
	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
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:

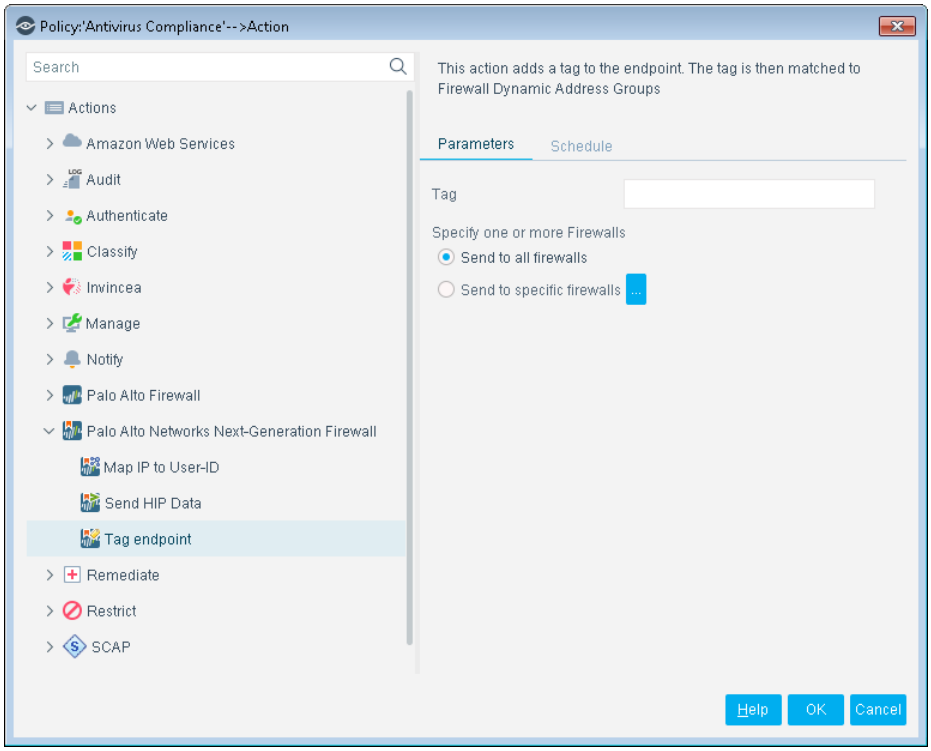
Send to all firewalls	Send HIP data to all firewall servers.
Send to specific firewalls	A list of target firewall servers. One or more can be selected.

Tag Endpoints

This action adds a tag to an endpoint. The tag is then matched to 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 will handle. The tag comprises logical *and* and *or* operators for defining the filtering criteria. CounterACT 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. Refer to Prepare Your Security Policy - Create a Dynamic Address Group.



The following parameters are available for selection:

Tag	Tag set up 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	A list of target firewall servers. One or more can be selected.

Using Palo Alto Networks NGFW Module

This section covers the best practices of using the Palo Alto Networks NGFW Extended Module.

Best Practices

- Once the Palo Alto NGFW Extended Module is configured, CounterACT will be able to include the actions of Map IP to User-ID, Send HIP Data, and Tag endpoint in policies affecting endpoints. In each case, administrators are able to elect whether or not 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 along to the Palo Alto firewall. This is particularly important in environments where the Palo Alto Global Connect client is either 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.
- Where Palo Alto segments or controls traffic based upon compliance status of endpoints, CounterACT 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 that require endpoints that are out of compliance to not be allowed to connect to resources where sensitive personal, financial, or health information is stored.
- For CounterACT to get the most out of the *Tag Endpoint* action, tags need to be first defined on the Palo Alto NGFW. These tags will have operators for determining which endpoints should be considered for each tag; CounterACT will then take those criteria and apply the tags appropriately across the enterprise.

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

General Guidance

- Consider the mapping of CounterACT appliances to Palo Alto firewalls. If both types of these 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, then consider expediting the flow of information from the CounterACT system 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 CounterACT responsible for endpoints in Region A would be best suited to communicate with that firewall. A CounterACT 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 HA. Cluster groups will not transfer communication responsibilities from one CounterACT to another. This is because each appliance will have its own keys used for communications with Panorama and Palo Alto NGFWs; these keys are non-transferable.

Access the Asset Inventory

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

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

To access the inventory:

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

If you did not configure to show the property in the Asset Inventory tab, your Palo Alto Networks NGFW properties will not display in the Views pane of the Asset Inventory tab.

3. Check that the properties match the configuration requirements.

Access the Home Tab

To access the Home tab:

1. In the CounterACT Console, select the **Home** tab.
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 *CounterACT CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT Inventory.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

> *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

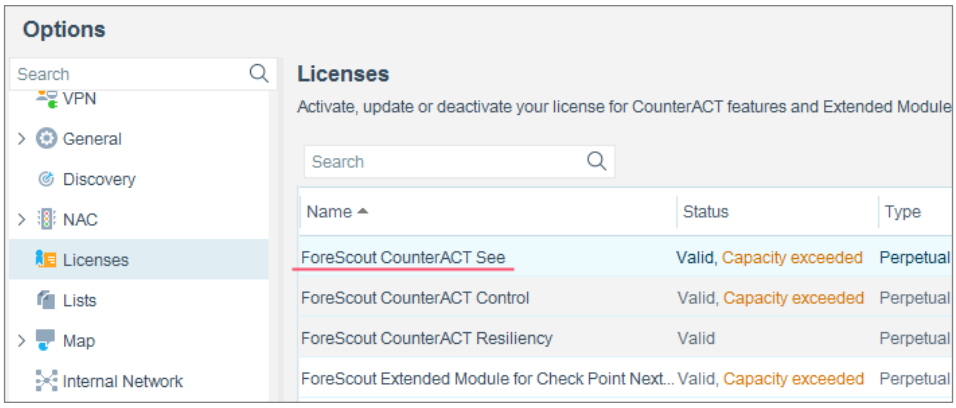
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-27 19:20