ForeScout

CounterACT™ Palo Alto Networks Firewall Plugin

Configuration Guide

Version 1.0.2 and Above

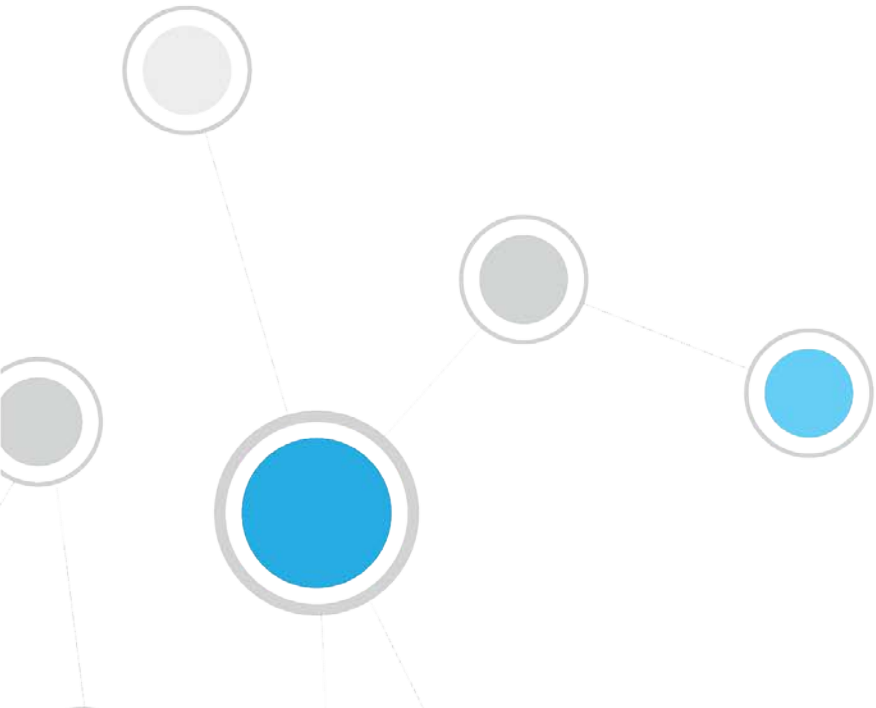


Table of Contents

About the Palo Alto Networks Firewall Plugin

The Palo Alto Networks Firewall Plugin lets you integrate CounterACT with Palo Alto Networks firewalls so that you can:

- Map host IP addresses discovered by CounterACT to firewall User-IDs. For example, the plugin can map the IP address of a user authenticating to a captive portal through a proxy. See Map IP to User-ID.
- Register host IP addresses discovered by CounterACT to a dynamic address object in a firewall. See Register To Dynamic Address Object.
- Use the CounterACT inventory to display Dynamic Address Objects that contain hosts registered by the plugin and a list of the registered hosts. See Displaying Palo Alto Networks Inventory Data.
- Create CounterACT reports that provide detailed information about endpoints impacted by the *Map IP to User-ID* and *Register to Dynamic Address Object* actions. For example you can create a Policy Details Report to display host details for custom policies containing these actions.

Refer to the *CounterACT Console User Manual* for more information about the inventory and report features.

To use the plugin, you should have a solid understanding of Palo Alto Networks firewall concepts, functionality and terminology, and understand how CounterACT policies and other basic features work.

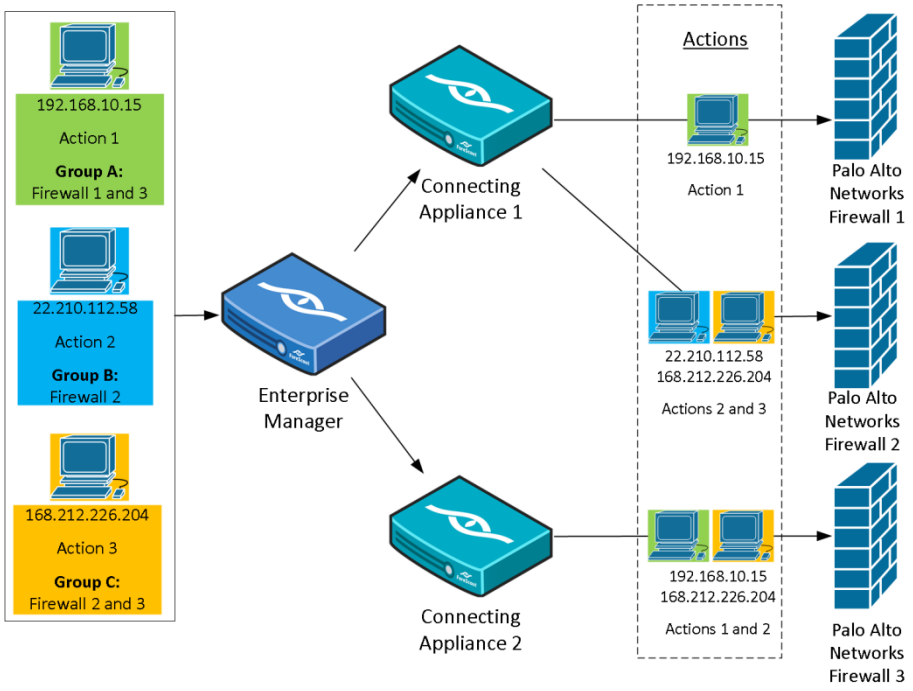
How it Works

The plugin communicates with Palo Alto Networks firewalls, supplying host IP information discovered by CounterACT. This information is directed to firewalls using the CounterACT *Map IP to User-ID* and *Register to Dynamic Address Object* actions.

Multiple firewall devices are classified into firewall groups. A firewall device can belong to more than one group. The plugin directs the actions to firewall devices according to the firewall group defined in each action.

Each firewall is assigned to a connecting CounterACT device which it communicates with. Multiple firewalls can be assigned to a single CounterACT device. The Enterprise Manager distributes actions to the relevant connecting CounterACT device, depending on the firewall group defined in the action. The connecting CounterACT device then sends the action to the relevant firewall.

Multiple connecting CounterACT devices can queue and handle the same action if the action is assigned to multiple firewall devices.



In order to efficiently manage communication between the plugin and firewalls, the plugin will add hosts triggered by the *Map IP to User-ID* or *Register to Dynamic Address Object* actions to a queue and send them to the firewall in one API call instead of sending each host immediately. You can configure the time to wait for new hosts and the number of hosts to queue before sending an API call in the plugin. See Configure General Firewall Options.

> *Dynamic address object updates are queued into 60-second intervals by Palo Alto Networks to prevent excessive updates to the firewall. If multiple changes are requested via the API in a 60 second cycle, they will all take place at the same time at the end of the cycle.*

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See Requirements.
- Download and install the plugin. See Install the Plugin.
- Configure settings in Palo Alto Networks firewalls. See Configure Settings in the Palo Alto Networks Platform.
- Define firewall details and plugin settings. See Configure the Plugin.
- Configure the *Map IP to User-ID* and *Register to Dynamic Address Object* actions. See Palo Alto Networks Firewall Policy Actions.

Requirements

- CounterACT version 7.0.0, running its latest hotfix.
- PAN-OS version 5.0, 6.0.x, 6.1.x and 7.0.x

> *If you are working with Dynamic Object actions, it is recommended that you use PAN-OS version 6.0 or above, which supports adding up to 10,000 IP addresses to a dynamic address object. PAN-OS version 5.0 only supports 256 IP addresses.*

Install the Plugin

This section describes how to download and install the plugin.

To download and install the plugin:

1. Navigate to the Customer Support Plugins page.
2. Save the plugin installation file to the machine where the CounterACT Console is installed.
3. Log in to the Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**.
6. The Open dialog box opens. Navigate to the location where you saved the plugin installation file and select **Install**.

Configure Settings in the Palo Alto Networks Platform

You need to make the following configurations in the Palo Alto Networks platform before you can integrate firewalls with the plugin.

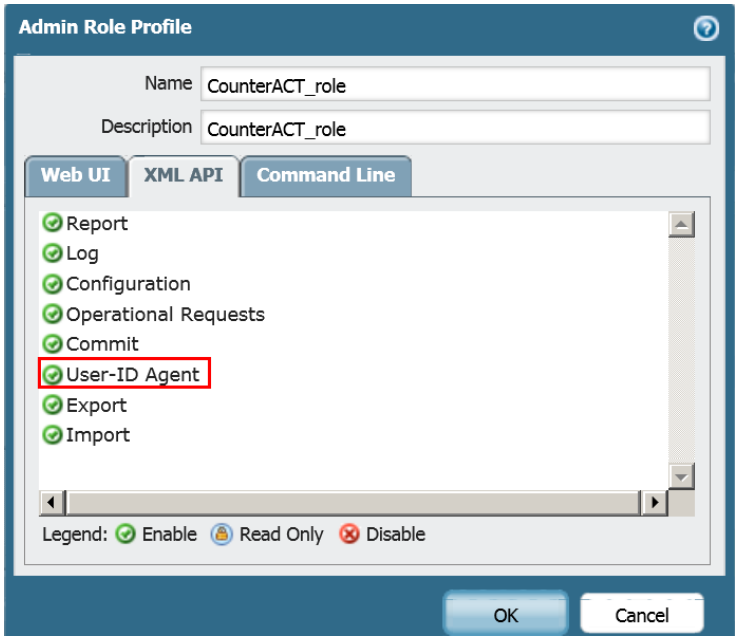
- Configure Account Settings
- Create a Dynamic Address Object

Configure Account Settings

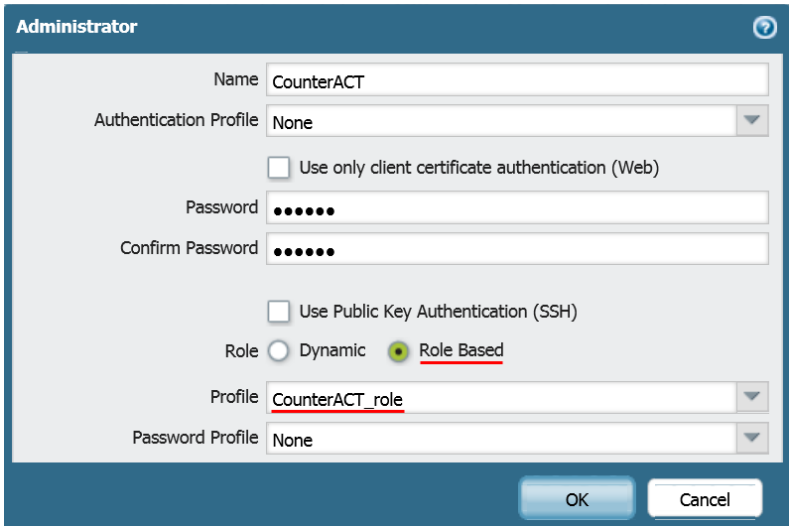
Before you configure a firewall in the plugin, you must ensure that the firewall has an administrator user with an XML API role assigned to it in the Palo Alto Networks platform. You will need to use these account credentials when you configure a firewall in the plugin.

To configure account settings:

1. In **Device > Admin Roles**, configure a role profile with the XML API – User-ID Agent permission enabled.



2. In **Device > Administrators** add an Administrator user and assign the user the previously created role profile.



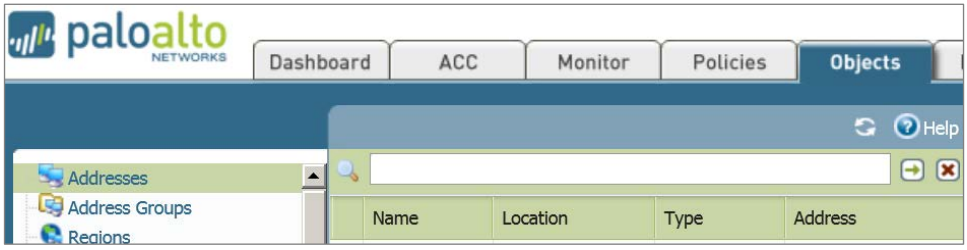
Create a Dynamic Address Object

Hosts detected by CounterACT that are triggered by the *Register to Dynamic Address Object* action are sent to the Dynamic Address Object. The Dynamic Address Object type is listed with the other object types.

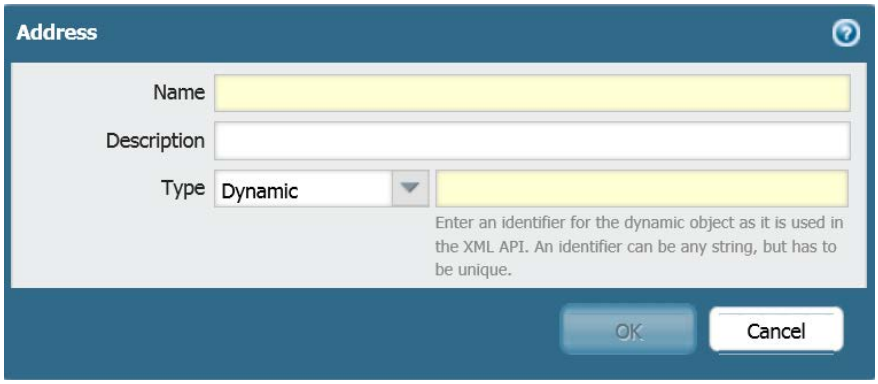
To use this action, you must create a Dynamic Address Object in the Palo Alto Networks platform.

To configure a Dynamic Address Object:

1. Select the **Objects** tab and then select **Addresses**.



2. Select **Add** and give the dynamic address object a name. Under Type, select **Dynamic**.



3. Enter an identifier for the dynamic object as it is used in the XML API. An identifier can be any unique string.

   You can use the name of the object in Palo Alto Networks policies. The identifier is used to map the unique IP address to an address object in the API script.

In PAN-OS 5.0 you can add up to 256 IP addresses to a dynamic address object. In PAN-OS 6.0 and above you can add up to 10,000 IP addresses to a dynamic address object.

Configure the Plugin

You can configure firewalls and firewall groups in the plugin to allow CounterACT devices to synchronize with and provide information to Palo Alto Networks firewalls. Before you configure a firewall in CounterACT, you must ensure that the firewall has an administrator user with the required XML API permissions. See Configure Account Settings.

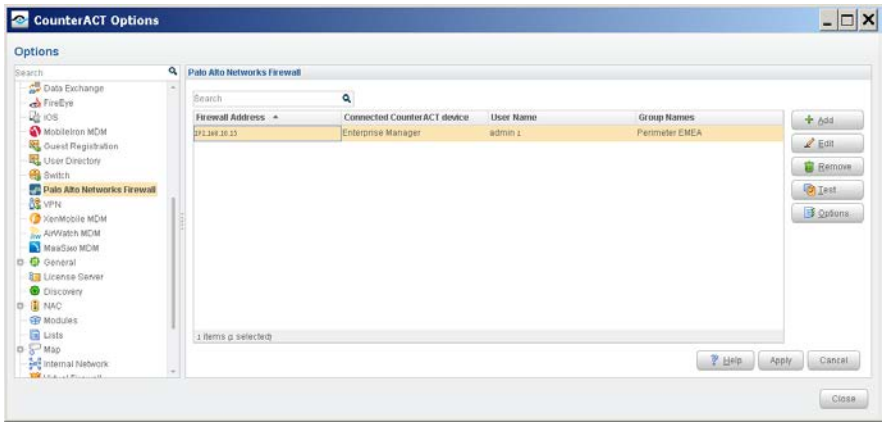
You can also configure firewall threshold settings. See Configure General Firewall Options.

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

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

To configure the plugin:

1. Select **Options** from the **Tools** menu and then select the **Plugins** folder.
2. In the **Plugins** pane, select the Palo Alto Networks Firewall Plugin and select **Configure**.

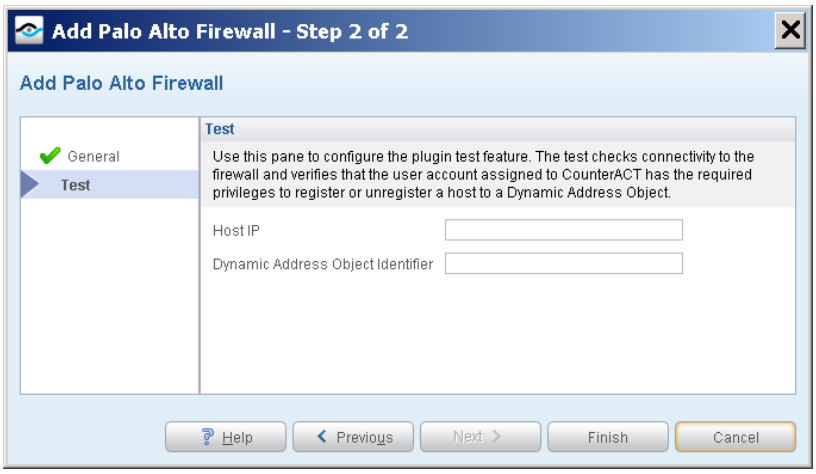


3. In the Palo Alto Networks Firewall pane, select **Add**. The Add Palo Alto Firewall dialog box opens.

4. In the **General** pane, configure the following connection parameters:

Firewall Address	IP address or domain name of a Palo Alto Networks firewall that will be the recipient of CounterACT actions.
PAN OS Version	The version of the Palo Alto Networks platform. The plugin supports PAN OS versions 5.0, 6.0 and 7.0.
User Name	User name for accessing the firewall. This user must have an XML API role.
Password	Password for the above user. Retype the password to confirm.
Connected CounterACT Device	Select the CounterACT device to communicate with the defined Palo Alto Networks firewall. The connected CounterACT device manages all communication with the defined firewall and forwards actions submitted to it by other CounterACT devices.
Group Names	Select one or more firewall group names for this firewall. Firewall groups are used to join multiple firewall devices together and to define firewall recipients in the *Map IP to User-ID* and *Register to Dynamic Address Object* actions. A firewall can belong to more than one group, but each firewall must belong to at least one group. When you configure actions, you must choose only one group as a recipient. CounterACT will communicate the action to all firewalls defined in the group.

5. Select **Next**. The **Test** pane opens.



The test checks connectivity to the firewall and verifies that the user account assigned to CounterACT has the required privileges to register or unregister a host to a Dynamic Address Object.

See Test the Plugin Configuration for information about running the test.

In the **Test** pane, configure the following parameters.

Host IP	The IP address of a host, used to test the connectivity of the plugin.

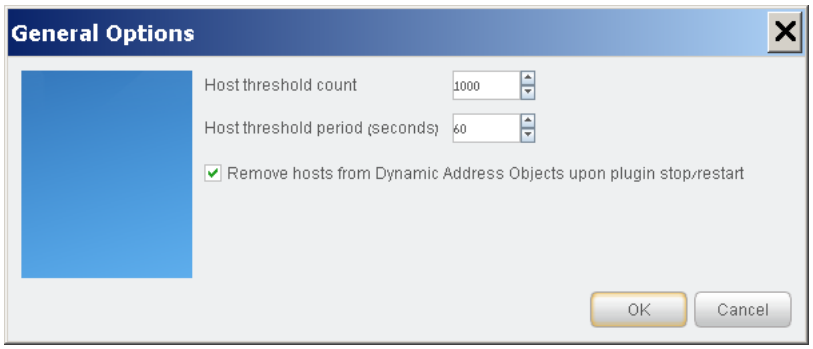
Dynamic Address Object Identifier	The identifier of the Dynamic Address Object, as configured in the Palo Alto Networks Platform. An identifier can be any unique string. It is used by the XML API to feed in addresses to the object.

6. Select **Finish**. The firewall appears in the Palo Alto Networks Firewall pane.

Configure General Firewall Options

You can configure Firewall options to determine when API calls are sent from the plugin to the firewall and when hosts are removed from Dynamic Address Objects.

1. In the Palo Alto Networks Firewall pane, select **Options**. The General Options dialog box opens.



2. Configure the following parameters:

Host Threshold count	The number of hosts to queue before sending an API call to the firewall. The default value is 1000 host requests.
Host Threshold period	The time to wait for new hosts before sending an API call to the firewall, in seconds. The default value is 60 seconds.
Remove hosts from Dynamic Address Objects upon plugin stop/restart	Select the checkbox to remove hosts from dynamic address objects upon plugin stop or restart. When selected, the plugin will clear all dynamic address object entries that were added through the Appliance that is being configured. If you clear the checkbox, the plugin will not remove dynamic address object entries when the plugin is stopped or restarted, unless you manually clear entries using the **`fstool pan clear objects`** command. See Clear Dynamic Objects from Firewall for details. This option is enabled by default.

3. Select **OK**.

Retrieve Deleted Firewall Configurations

You can restore deleted firewall settings for firewalls that were removed from the Palo Alto Networks Firewall pane as long as the changes have not yet been applied.

To retrieve deleted firewall configurations:

1. After one or more firewalls were removed from the Palo Alto Networks Firewall pane, select **Cancel** to revert to the last saved configuration.

   Configuration settings are only saved when you select **Apply**.

Test the Plugin Configuration

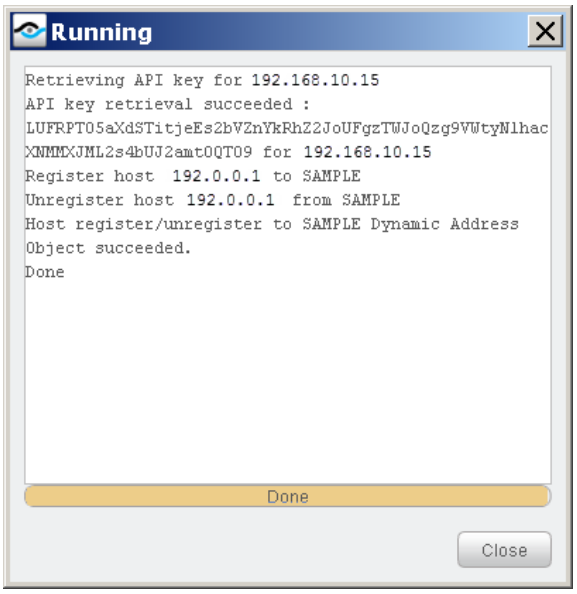
This section describes how to perform a configuration test.

The test checks connectivity to the firewall and verifies that the user account assigned to CounterACT has the required privileges to register or unregister a host to a Dynamic Address Object. This ensures that the *Register to Dynamic Object* action works properly.

The test is performed independently for each firewall.

To run a test:

1. Verify that you have properly configured test settings in the firewall. See Configure the Plugin.
2. In the Palo Alto Networks Firewall pane, select the firewall you want to test and select **Test**.



3. Select **Close**.

Clear Dynamic Objects from Firewall

You can run a ForeScout fstool command on CounterACT devices to clear dynamic objects from the firewall.

To clear specific dynamic objects from the firewall:

1. Log on to the CounterACT device as root.
2. Run the following command:

   fstool pan clear_objects -device <IP address/DNS> -objects <dyanmic object identifier> [<dynamic object identifier>

   Or using the abbreviated form:

   fstool pan clear_objects -d < IP address/DNS> -o <dyanmic object identifier> [<dynamic object identifier>

   For example:

   fstool pan clear_objects -d 192.168.10.15 -o non_compliance

Create Custom Palo Alto Networks Policies

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 hosts 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 Firewall plugin related actions to create custom policies. These items are available when you install the plugin.

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 Firewall Policy Actions

This section describes the actions that are made available when the Palo Alto Networks Firewall plugin is installed.

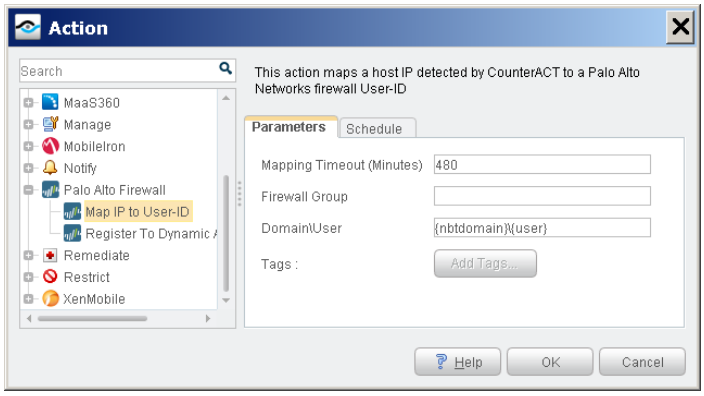
To access Palo Alto Networks Plugin actions:

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the Palo Alto Networks folder in the Actions tree. The following actions are available:
   - Map IP to User-ID
   - Register To Dynamic Address Object

Map IP to User-ID

This action lets you map a host IP detected by CounterACT to a Palo Alto Networks firewall User-ID. CounterACT must be able to detect a fully qualified domain name (FQDN) to map a host IP.

Palo Alto Networks firewalls employ a User Identification (User-ID) feature to configure and enforce firewall policies based on users and user groups. 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 plugin leverages CounterACT advanced endpoint detection capabilities to identify and contribute user information to firewalls.



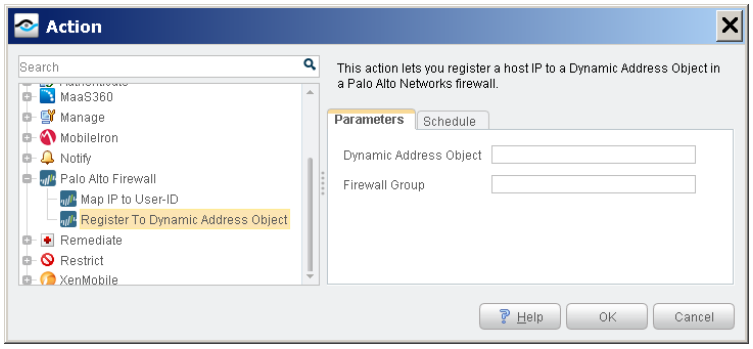
The following parameters are available:

Mapping Timeout	The amount of time that the action persists in the firewall, in minutes.
Firewall Group	The target firewall group that the action is applied to. Enter a group you defined when configuring the plugin. Names are case sensitive. See Configure the Plugin. A firewall group is a collection of one or more firewall devices. Each firewall must be assigned to at least one group.
Domain and User	By default, this parameter consists of the *nbtdomain* and *user* property tags representing the NetBIOS domain and the user name. You can edit this parameter, but you need to verify that the values reflect the User-ID Agent settings in your Palo Alto Networks Firewall.

Register To Dynamic Address Object

This action lets you register a host IP detected by CounterACT to a Dynamic Address Object in a Palo Alto Networks firewall.

Dynamic address objects are an address object type used to apply a predefined firewall policy to a group of hosts. By registering hosts to dynamic address objects, the plugin can share CounterACT host IP addresses with firewalls. For example, a host classified as non-compliant in CounterACT that is registered to a dynamic address object would also be considered as such in the firewall.



The following parameters are available:

Dynamic Address Object Identifier	The identifier of the Dynamic Address Object, as configured in the Palo Alto Networks Platform. An identifier can be any unique string. It is used by the XML API to feed in addresses to the object.
Firewall Group	The target firewall group that the action is applied to. A firewall group is a collection of one or more firewall devices. Each firewall must be assigned to at least one group. See Configure the Plugin.

Displaying Palo Alto Networks Inventory Data

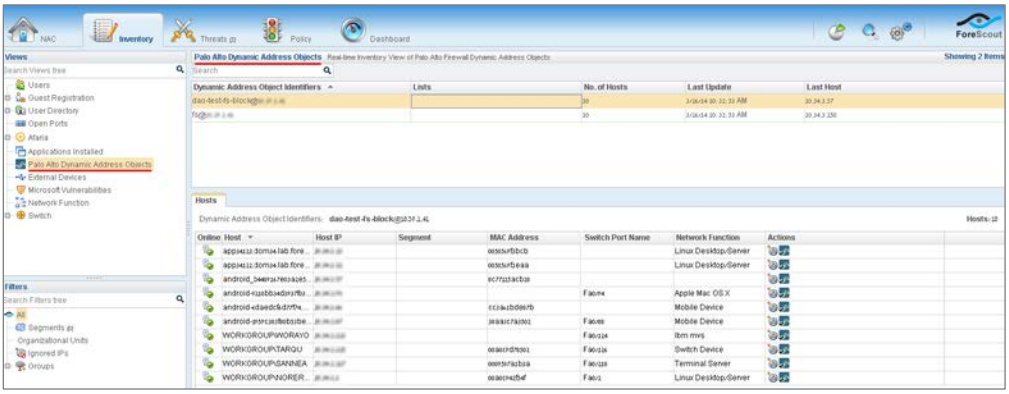
Use the CounterACT Inventory to view a real-time display of Palo Alto Networks network activity at multiple levels.

The inventory lets you:

- Broaden your view of the organizational network from endpoint-specific to activity-specific
- View endpoints that have been detected with specific attributes
- Easily track network activity
- Incorporate inventory detections into policies

To access the inventory:

1. Select the Inventory tab from the Console toolbar.
2. Navigate to the Palo Alto Dynamic Address Objects entries.



The following information, based on Palo Alto Networks endpoint properties, is available:

- Palo Alto Dynamic Address Objects: View all dynamic address object identifiers and the number of hosts that are registered to each.

Refer to *Working at the Console>Working with Inventory Detections* in the *CounterACT Console User Manual* or the Console, Online Help for information about how to work with the CounterACT Inventory.

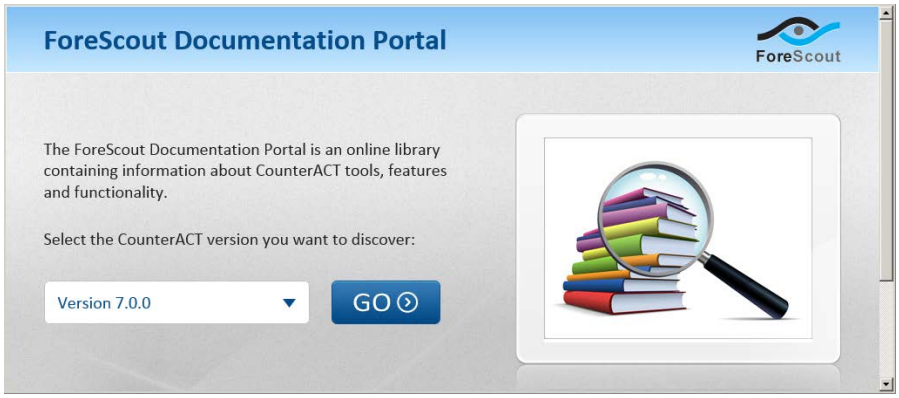
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, you can refer to the following resources:

- Documentation Portal
- Customer Resource Center
- CounterACT Console Help Tools

Documentation Portal

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



To access the Documentation Portal

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

Customer Resource Center

The Customer Resource Center provides links to CounterACT version releases, Hotfixes, Plugins and Module as well as related documentation. The center also provides a variety of How-to Guides, Installation guides and more.

To access the Customer Resource Center:

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

CounterACT Console 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.

Console User Manual

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

Plugin Help files

1. Select **Options** from the **Tools** menu and the select **Plugins**.
2. Select a plugin and then select **Help**.

Documentation Portal

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

Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2016. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2016-06-30 14:28