ForeScout® Extended Module for Palo Alto Networks® Wildfire

Configuration Guide

Version 2.1

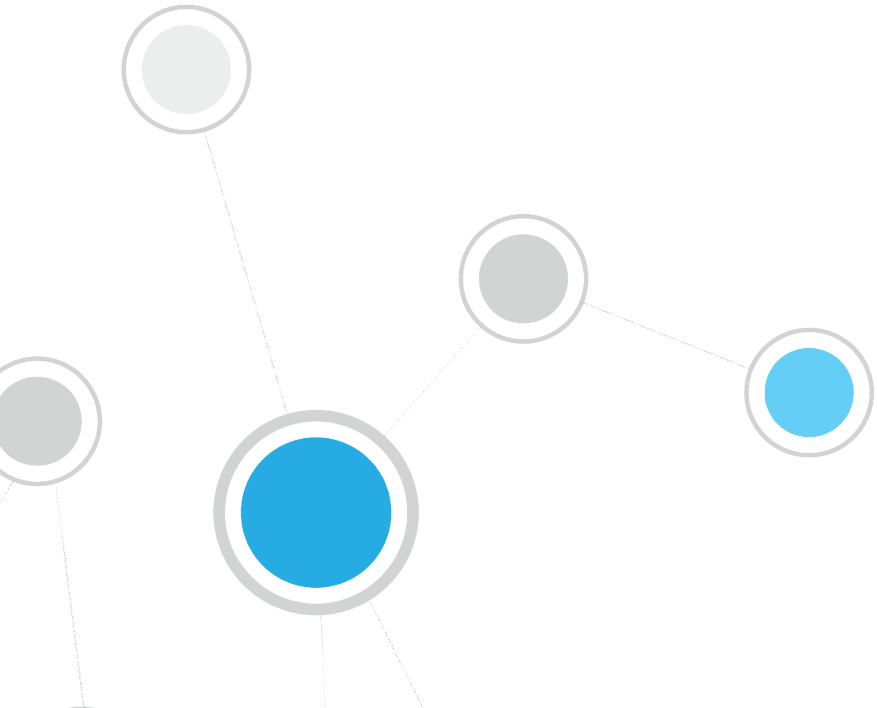


Table of Contents

About the Palo Alto Networks WildFire Integration

The Palo Alto Networks Wildfire Module, together with the IOC Scanner Plugin, integrates CounterACT with Palo Alto Networks WildFire. This integration combines the threat detection mechanisms of Palo Alto Networks WildFire with the network visibility and compliance enforcement capabilities of CounterACT to multiply the benefits of working with an Advanced Threat Detection product.

The Palo Alto Networks WildFire Module enables ForeScout CounterACT® and Palo Alto Networks WildFire to work together to quickly find indicators of compromise (IOCs), detect advanced threats, contain infected endpoints and disrupt the cyber kill chain preventing further lateral threat propagation and data exfiltration. This allows the security team to prevent, detect, analyze and respond to today's advanced attacks.

Advanced Threat Detection with the IOC Scanner Plugin

This module works with the IOC Scanner Plugin – CounterACT's action center for Advanced Threat Detection (ATD) and response. The IOC Scanner Plugin provides:

- A centralized repository of all threats and their IOCs (indicators of compromise) reported to CounterACT by third-party ATD solutions and other threat prevention systems, or added manually.
- Mechanisms that scan all Windows endpoints for threat and IOC information reported to CounterACT, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- **ATD Stage 1 (this module): Detect and report threats on endpoints:** Palo Alto Networks Firewall instances in your environment report threats to this module as they are detected on endpoints. Use the template provided with this module to create policies that apply restrictive CounterACT actions based on the severity of detected threats.

  In addition to this initial response, all threats reported by this module are automatically submitted to the IOC Scanner Plugin, which parses the threat to yield indicators of compromise (IOCs) - measurable events or state properties that can be used as a "fingerprint" to identify the threat. The IOC Scanner Plugin uses these IOCs to mount further scan/analyze/remediate stages of CounterACT's ATD response, as follows:

- **ATD Stage 2 (IOC Scanner Plugin): Real-time hunt for endpoints of interest based on threats and IOCs:** The IOC Scanner Plugin detects endpoints with IOCs associated with recently reported threats.
- **ATD Stage 3 (IOC Scanner Plugin): Evaluation and remediation:** The IOC Scanner Plugin evaluates the profile of IOCs on endpoints of interest to determine the likelihood that an endpoint is compromised, and applies appropriate blocking/remediation actions.

For more information about IOC-based threat detection and remediation, refer to the *IOC Scanner Plugin Configuration Guide*.

Use Cases

This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About This ModuleAbout This .

- Receive alerts from Palo Alto Networks of threats detected and immediately perform restrictive actions on the endpoints on which they were detected.
- Scan all Windows endpoints for IOCs reported to CounterACT by Palo Alto Networks WildFire in order to identify threats and perform actions on potentially infected endpoints. For example, use CounterACT policies to run policy actions that immediately:
  - Contain infected endpoints, for example limit or block network access. This prevents lateral movement of the infection to other endpoints.
  - Remediate infected endpoints, for example by killing suspicious processes.
  - Notify stakeholders by, for example, sending an email to corporate security teams with details about which threats were detected on which endpoints.

  For more detailed information about this use case, refer to the section about use cases in the *CounterACT IOC Scanner Plugin Configuration Guide*.

Additional Palo Alto Networks Documentation

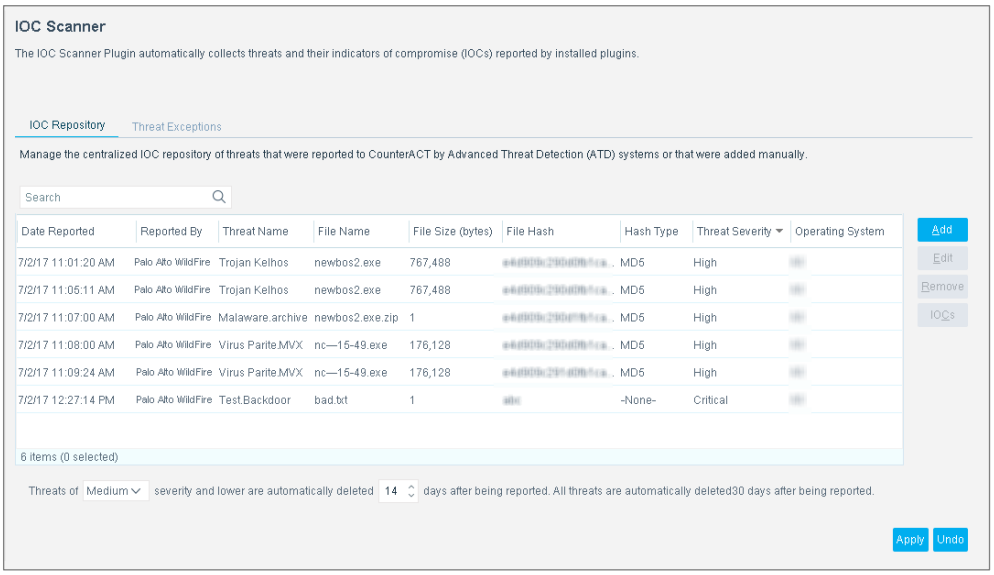
Refer to Palo Alto Networks online documentation for more information about the WildFire solution:

- PAN-OS Administrator's Guide Version 6.0
  https://live.paloaltonetworks.com/docs/DOC-6603
- WildFire Administrator's Guide Version 6.0
  https://live.paloaltonetworks.com/docs/DOC-6589

About This Module

This module, together with the IOC Scanner Plugin, lets you integrate CounterACT with Palo Alto Networks WildFire so that you can:

- Use the ATD Stage 1: Palo Alto Networks WildFire Threat Detections policy template to create policies that immediately run appropriate actions, such as restrictive actions, on endpoints on which Palo Alto Networks WildFire detected a Critical or High severity threat.
- Create Custom Palo Alto Networks WildFire Policies that use Palo Alto Networks WildFire – Policy Properties alongside other CounterACT properties and actions to deal with issues not covered in the *ATD Stage 1: Palo Alto Networks WildFire Threat Detections* policy template.
- View new IOCs related to threats reported by Palo Alto Networks WildFire and automatically added to the IOC repository. Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for more information.



- Use CounterACT inventory tools to display all threats reported by Palo Alto Networks WildFire in the last 30 days and the endpoints for which WildFire reported them. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how the threat has moved through your network.

To use the module, you should have a solid understanding of Palo Alto Networks WildFire concepts, functionality and terminology, including an understanding of how to leverage threat intelligence distributed by IOCs. You should also understand how CounterACT policies and other basic features work.

How It Works

When a threat is detected, the Palo Alto Networks Firewall sends an alert with the threat details to a pre-defined receiving CounterACT device. The Palo Alto Networks Firewall only sends alerts to CounterACT about threats determined to be *malicious*. The alert includes:

- source/destination IP address
- timestamp of the event
- threat name, file name, severity and hash
- IOC details identified throughout the lifecycle of the threat on different operating systems (according to how Palo Alto Networks WildFire is configured in your environment), such as:
  - Process Names

    If the reported malicious process indication is an .exe file, the filename is stored in the IOC repository as both a *Process* IOC and a *File Exists* IOC. If the malicious process indication is a loaded .dll file, the filename is stored as a *File Exists* IOC only. CounterACT detects .dll or .exe Portable Executable file types only.
  - File Names
  - Registry Keys and Values
  - Service Names
  - DNS Queries

– Command and Control (CnC) URLs

CounterACT adds the data to its IOC repository, and resolves the data as CounterACT properties associated with the endpoint on which the threat was discovered, as well as properties on other Windows endpoints. These properties can be used to trigger policy actions.

The IOC repository includes all the IOCs identified by Advanced Threat Detection systems throughout a threat's lifecycle. CounterACT can use this information to detect the same threat on other endpoints. For example, CounterACT can scan endpoints not protected by Palo Alto Networks WildFire, detect IOCs used during a threat infection phase, and trigger a threat remediation action.

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.

Refer to the *CounterACT IOC Scanner Plugin Configuration Guide* for details.

What to Do

You must perform the following to work with this module:

1. Verify that you have met system requirements. See Requirements.
2. Configure the Palo Alto Networks Firewall.
3. Install the Module.
4. Configure the Module.
5. Run the Palo Alto Networks WildFire Policy Template (optional).
6. Create Custom Palo Alto Networks WildFire Policies (optional).

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- Palo Alto Networks Requirements

CounterACT Software Requirements

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

- CounterACT version 8.0.
- Core Extensions Module version 1.0 or above with the following components running (see Core Extension Module Information):

- Syslog Plugin
- IOC Scanner Plugin

ForeScout Extended Module License Requirements

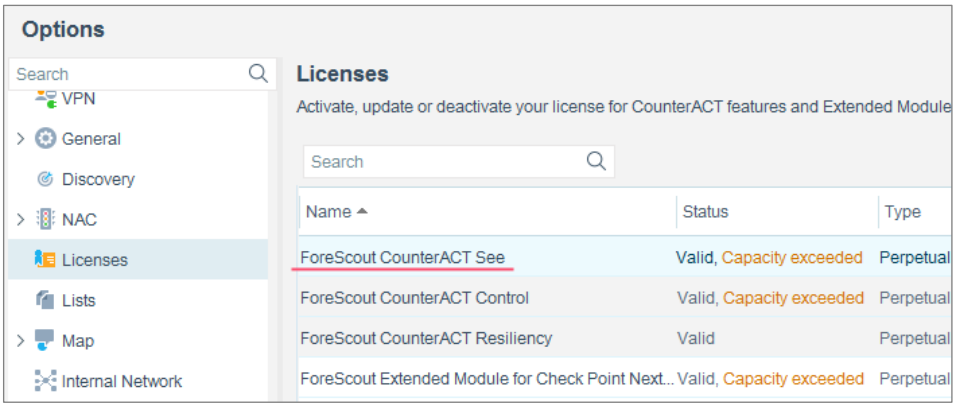
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- 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 Requirements

The module requires Palo Alto Networks Firewall running one of the following versions of PAN-OS, with a valid WildFire license:

- 6.0.x
- 6.1.x
- 7.0.x
- 7.1.x

> *WildFire integration can be carried out with a public cloud based infrastructure or an on-premise solution.*

Configure the Palo Alto Networks Firewall

Verify that the Palo Alto Networks Firewall is running and configured in your environment, and perform the following steps.

- Enable the WildFire Module
- Configure Communication with CounterACT

Enable the WildFire Module

Verify that the WildFire module is enabled. This includes:

- Setting up a File Blocking profile to capture all files from any application type. This option is available from the Palo Alto Networks platform in **Objects > Security Profiles > File Blocking**. In PAN-OS 7.x.x, you must also set up a WildFire Analysis profile. This option is available from the Palo Alto Networks platform in **Objects > Security Profiles > WildFire Analysis**. Refer to Palo Alto Networks documentation for more information about setting up these profiles.

- (Recommended) Configuring Palo Alto Networks to send all file types to the WildFire server or cloud to be checked.

Configure Communication with CounterACT

In the Palo Alto Networks Firewall UI, define each connecting CounterACT device as a syslog server that will receive Palo Alto Networks WildFire syslog messages.

Use the default log format. Do not create a custom log format.

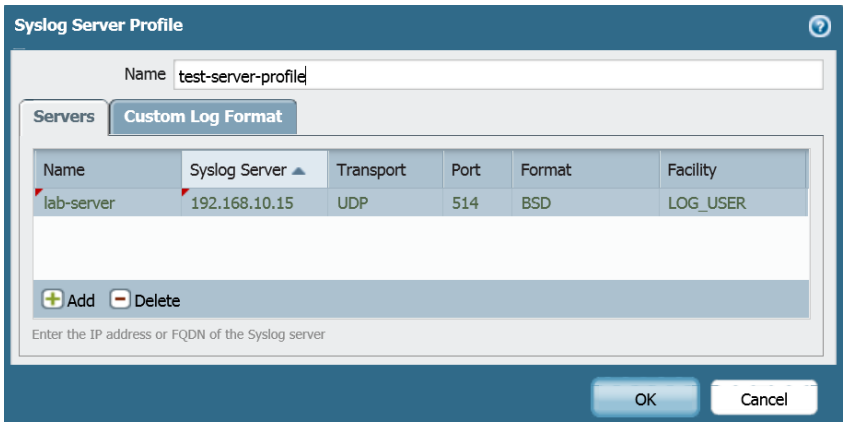
You can configure this communication per firewall or via Panorama. Panorama provides centralized monitoring and management of multiple Palo Alto Networks firewalls.

- Configure a Firewall
- Configure Panorama

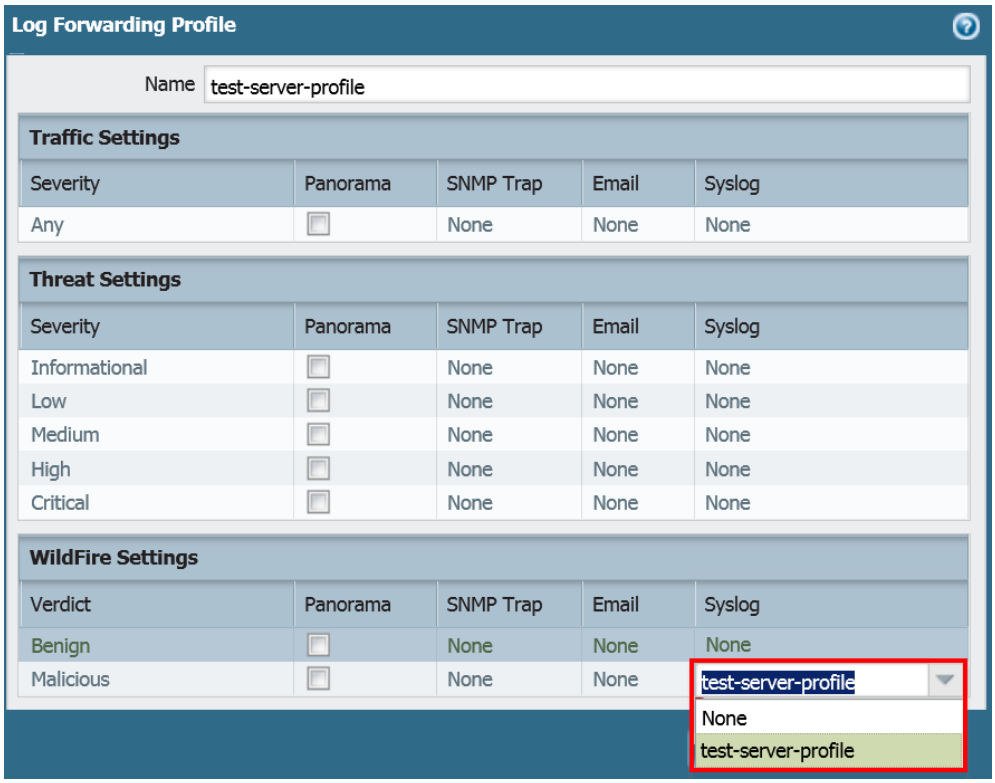
Configure a Firewall

To define a connecting CounterACT device as a syslog server:

1. In the Palo Alto Networks Firewall UI, create a syslog server profile:
   a. Select **Device** > **Server Profiles** > **Syslog** > **Add**. The Syslog Server Profile dialog box opens.



   b. Enter a unique name and the IP address of the connecting CounterACT device. Keep the default values for the Port, Format and Facility fields. The Transport field can be set to either UDP or TCP.
2. Create a Log Forwarding Profile and select the threat logs to be forwarded to the syslog server:
   a. Select **Objects** > **Log forwarding** > **Add**. The Log Forwarding Profile dialog box opens.



b. Enter a unique name for the profile.

c. In the Syslog column for Malicious threats, select the Syslog Server Profile to be used for forwarding threat syslog messages to the connecting CounterACT device.

Once configured, the log forwarding configuration should look similar to the following:

Name	Location	Log Type	Severity	To Panorama	SNMP Trap	Email	Syslog
test-server-profile		Threat					
		WildFire	malicious				test-server-profile
		Traffic					

3. Set the security rules using the Log Forwarding profile and a previously defined File Blocking profile that captures all files from any application type:

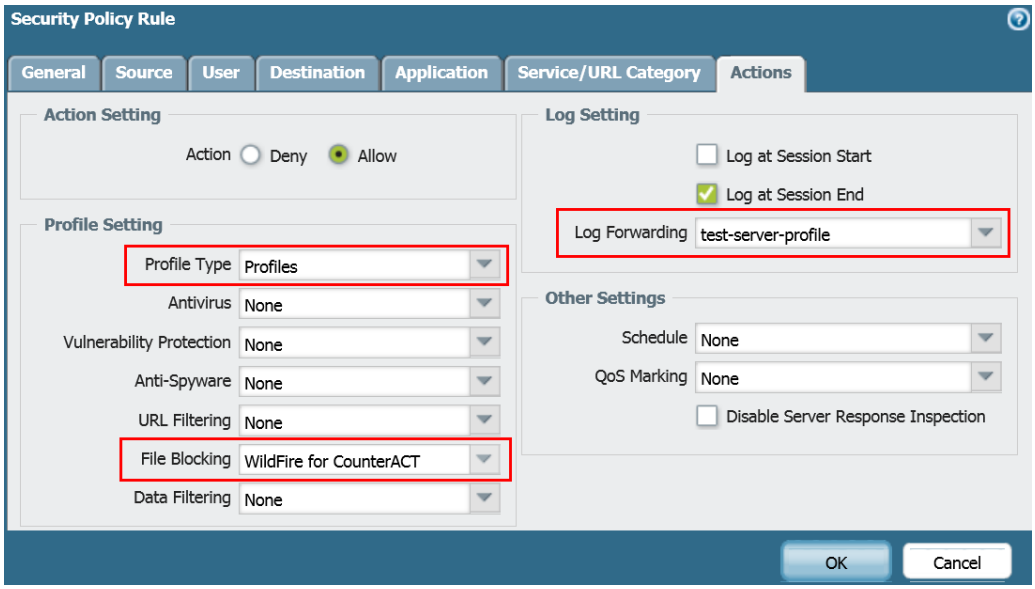
a. Select **Policies** > **Security Rule**.

b. Select the rule for which the log forwarding needs to be applied. Apply the security profiles to the rule.

c. Select **Actions**, and then select the following:

In the Log Setting area, select the *Log Forwarding* profile created in step 2 from the dropdown list.

In the Profile Setting area, select **Profiles** as the *Profile Type* and select the relevant *File Blocking* profile from the dropdown list.



In PAN-OS 7.x.x, select the relevant WildFire Analysis profile from the dropdown list in addition to the profiles listed above. The WildFire Analysis option will appear in the Profile Setting area.

d. Select **OK**.

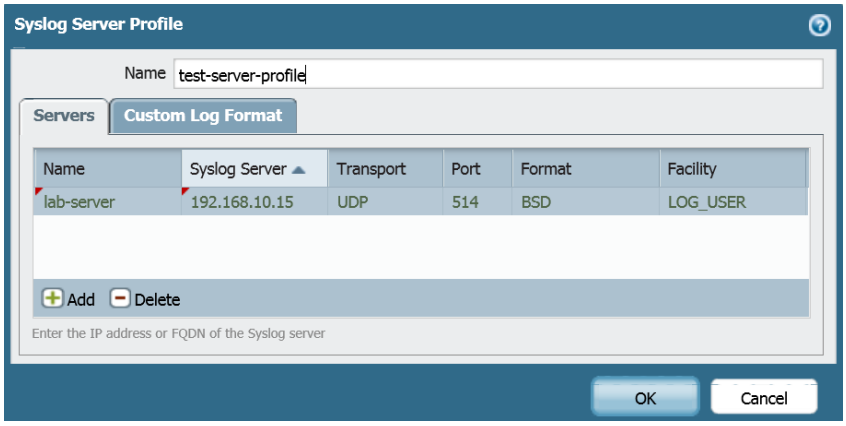
Configure Panorama

Panorama provides centralized monitoring and management of multiple Palo Alto Networks firewalls.

To define a connecting CounterACT device as a syslog server:

1. In the Palo Alto Networks Firewall UI, create a syslog server profile:

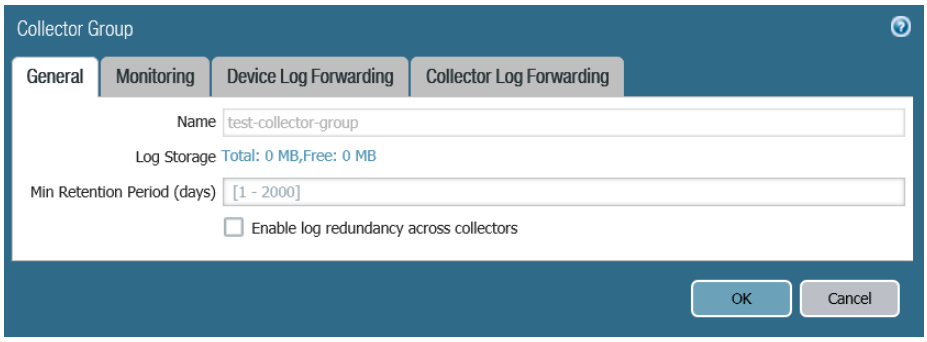
a. Select **Panorama** > **Server Profiles** > **Syslog** > **Add**. The Syslog Server Profile dialog box opens.



b. Enter a unique name and the IP address of the connecting CounterACT device. Keep the default values for the Port, Format and Facility fields. The Transport field can be set to either UDP or TCP.

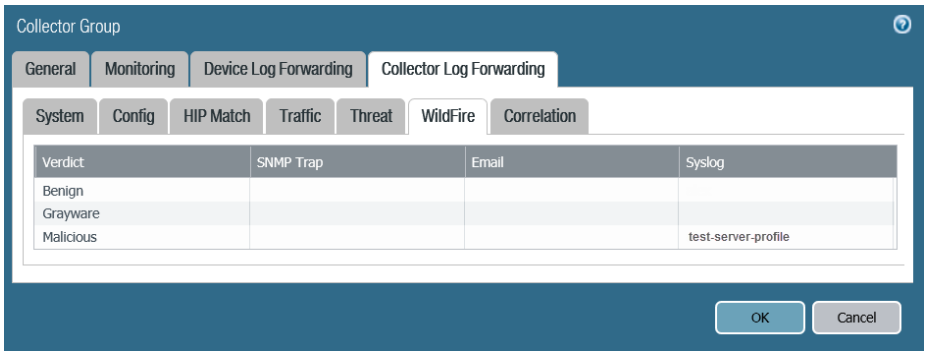
2. Assign the Syslog Server Profile to the various log types by creating a Collector Group:

   a. Select **Panorama > Collector Groups > Add**. The Collector Group dialog box opens.



   b. In the General tab, enter a name.

   c. Select **Collector Log Forwarding > WildFire**.



   d. In the Syslog column for Malicious threats, select the Syslog Server Profile to be used for forwarding threat syslog messages to the connecting CounterACT device.

Install the Module

This section describes how to install the module. Before you install this module, first install the IOC Scanner Plugin.

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.

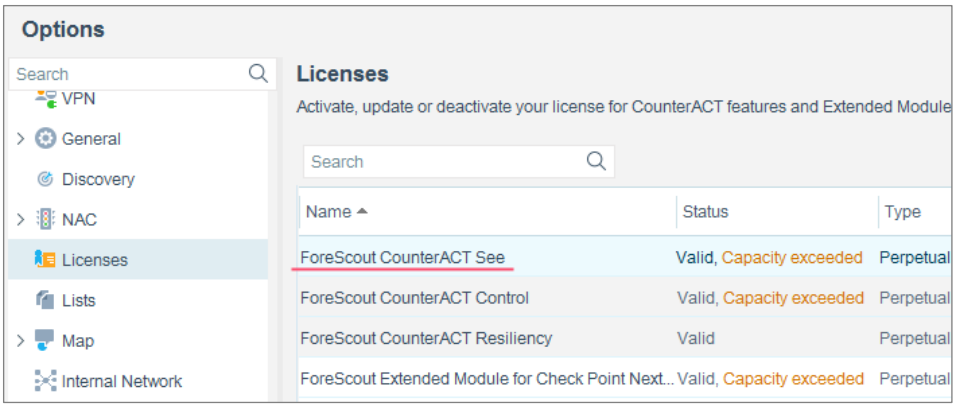
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    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.

Configure the Module

Configure the module for CounterACT to communicate with the WildFire service.

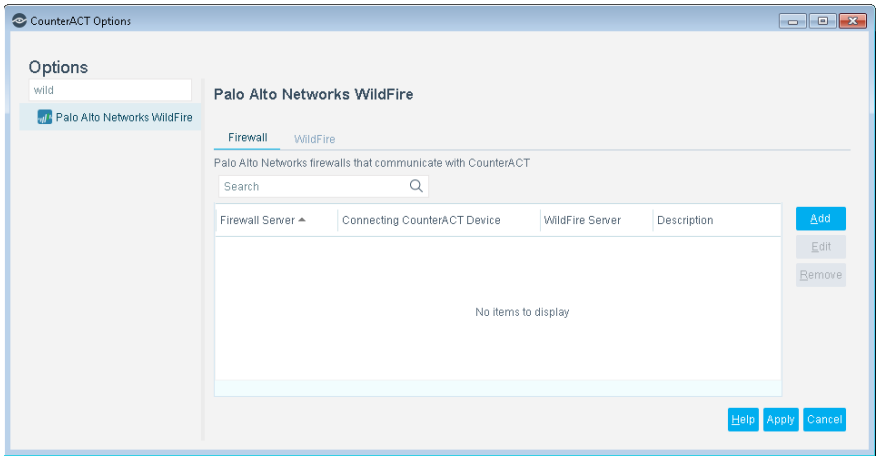
- Define each WildFire server and its login credentials. See Configure WildFire Servers.
- Define each Firewall server, including the name of a defined WildFire server and the CounterACT device it communicates with. See Configure Firewall Servers.

Configure WildFire Servers

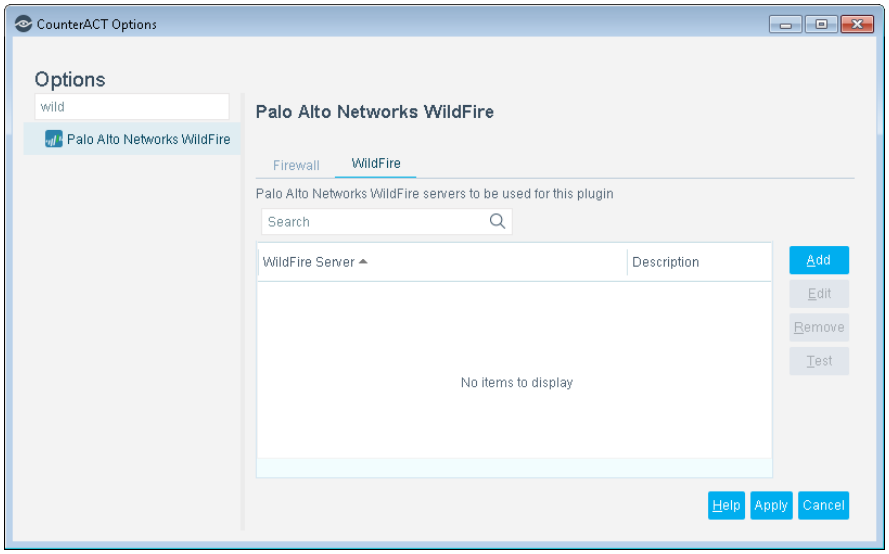
WildFire servers provide IOC details of the threats detected by Palo Alto Networks WildFire. Define each WildFire server and its login credentials.

To define WildFire servers:

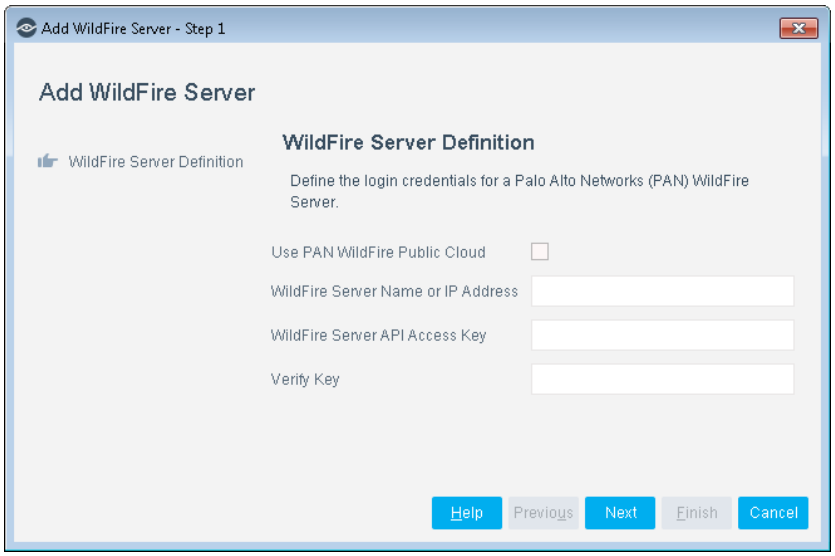
1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Modules** folder.
3. In the **Modules** pane, select **Palo Alto Networks WildFire**, and select **Configure**. The Palo Alto Networks WildFire pane opens.



4. Select the **WildFire** tab.



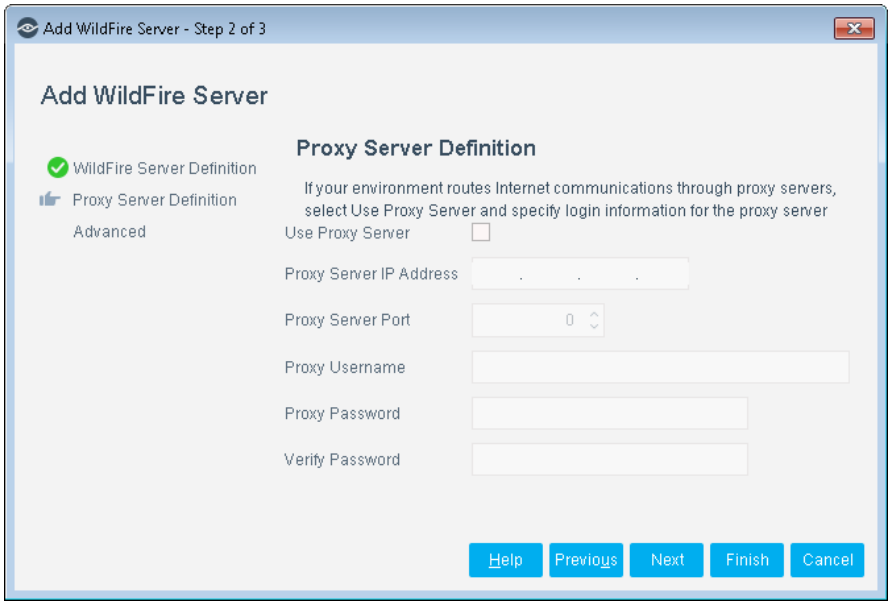
5. Select **Add** to define a Palo Alto Networks WildFire server that will provide IOC details of reported threats to CounterACT. The Add WildFire Server dialog box opens.



6. Enter the following information:

Use PAN WildFire Public Cloud	Determines if WildFire is in a public cloud. If selected, the server name automatically appears in the **WildFire Server Name or IP Address** field. *Verify that the Connecting CounterACT Device has access to the public cloud. CounterACT uses port 443 to communicate with WildFire. The Firewall and the WildFire public cloud use ports 443 and 10443 to communicate with each other.*
WildFire Server Name or IP Address	The server name or IP address of the WildFire server.
WildFire Server API Access Key	Login credentials to the WildFire server. Contact Palo Alto Networks for information on how to obtain this key.
Verify Key	Retype the key to confirm it.

7. Select **Next**. The Proxy Server Definition pane opens.



8. Enter the following information:

Use Proxy Server	Select this option to use a proxy server to communicate with PAN WildFire.
Proxy Server IP Address	The network address of the proxy server.
Proxy Server Port	The port used to communicate with the proxy server.
Proxy Username	Login name for an authorized account defined on the proxy server, if required.
Proxy Password	Password for the above user, if required.
Verify Password	Retype the password to confirm it.

9. Select **Next**. The Advanced pane opens.

10. Enter the following information:

Description	A textual description of the WildFire server. (Optional)

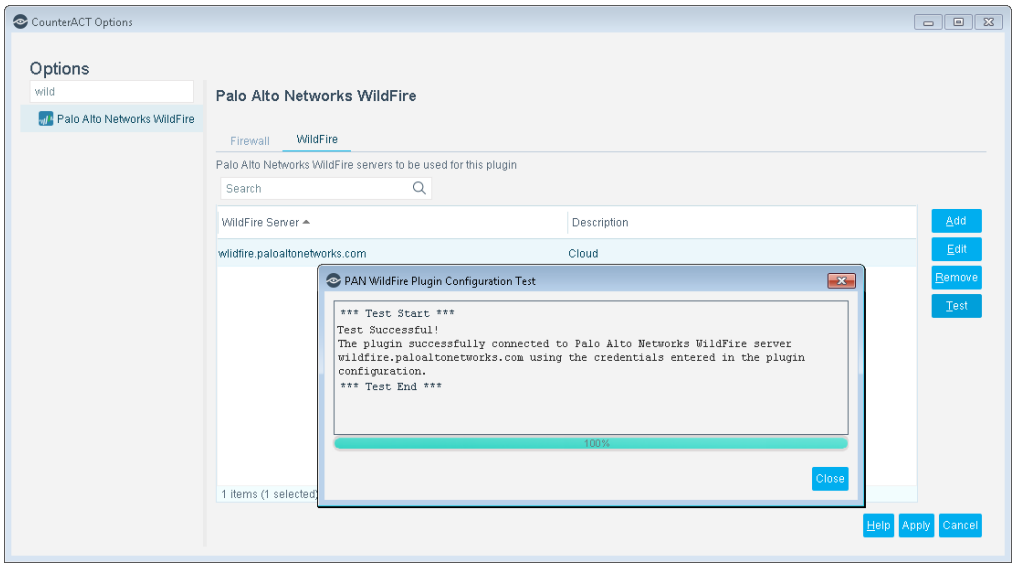
11. Select **Finish**.
12. Select **Apply** to apply the changes.

Test the WildFire Servers

Test each WildFire server configuration to ensure that the module can connect to it. Before testing a server, go to the Options > Modules pane, and ensure that the module is running on at least one CounterACT device.

To test a WildFire server:

1. In the WildFire tab, select the WildFire Server to be tested, and select **Test**. The test runs and the results are displayed.

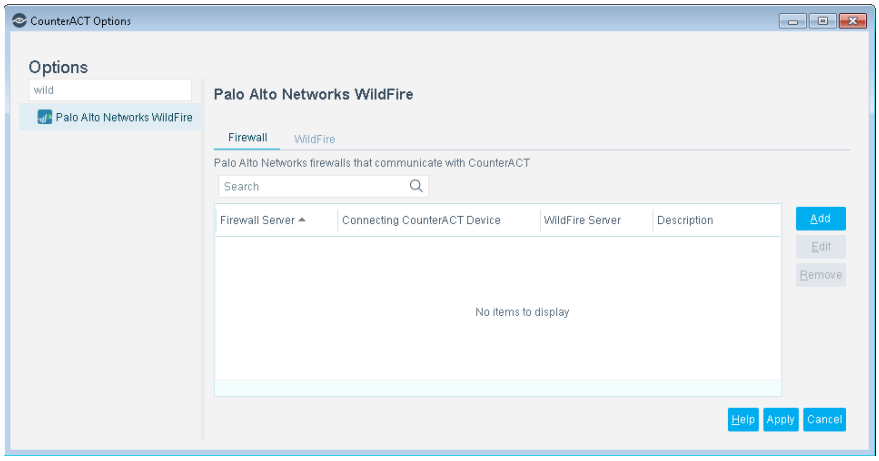


Configure Firewall Servers

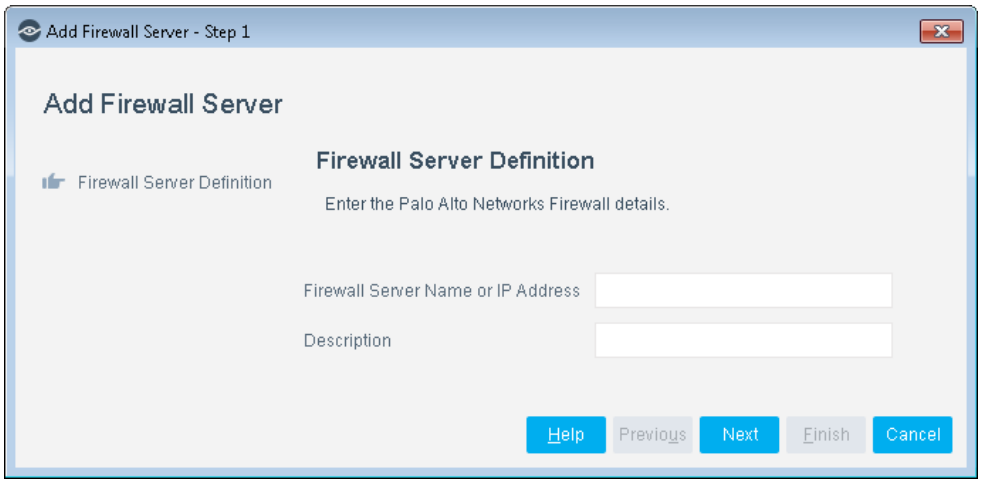
The Firewall sends the initial alert of detected threats to CounterACT. Define Firewall server information, along with information about the configured WildFire server and the CounterACT device that communicates with the WildFire server.

To define Firewall servers:

1. In the Palo Alto Networks WildFire pane, select the **Firewall** tab.



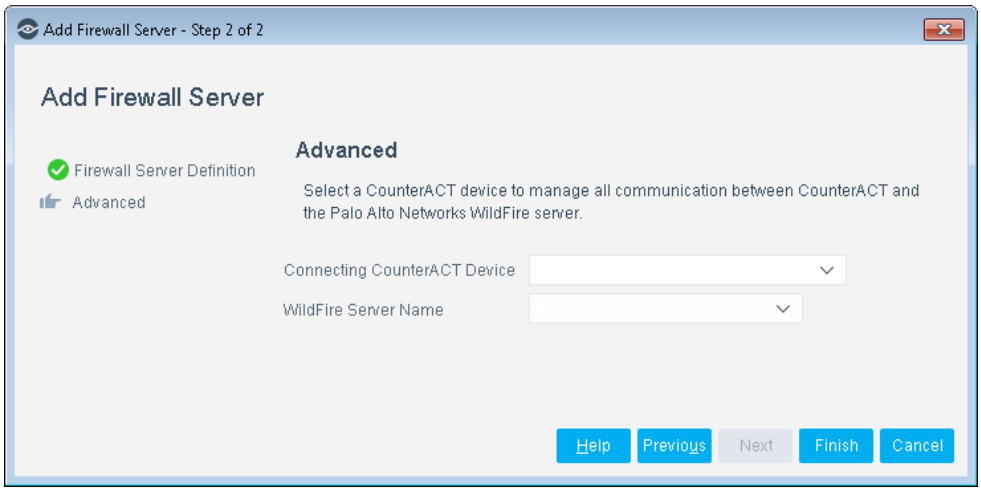
2. Select **Add** to define a Palo Alto Networks Firewall server to communicate with CounterACT. The Add Firewall Server dialog box opens.



3. Enter the following information:

Firewall Server IP Address	The IP address of the Firewall server.
Description	A textual description of the Firewall server. (Optional)

4. Select **Next**. The Advanced pane opens.



5. Enter the following information:

Connecting CounterACT Device	The IP address of the CounterACT device to communicate with the Firewall server. Connecting CounterACT devices must be defined to Palo Alto Networks as syslog servers. See Configure Communication with CounterACT for details.
WildFire Server Name	WildFire server defined in the Configure WildFire Servers section.

6. Select **Finish**.
7. Select **Apply** to apply the changes.
8. Navigate to and select the **Modules** folder.
9. In the **Modules** pane, select **Palo Alto Networks WildFire**, and ensure that the module is running on all connecting CounterACT devices configured in the Palo Alto Networks Firewall.

Run the Palo Alto Networks WildFire Policy Template

This module provides the following policy template which you can use to handle threats in a Palo Alto Networks WildFire environment.

- ATD Stage 1: Palo Alto Networks WildFire Threat Detections

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the CounterACT Administration Guide.

ATD Stage 1: Palo Alto Networks WildFire Threat Detections

Use this policy to identify the criticality of each discovered threat reported by Palo Alto Networks WildFire and then send a message to the syslog server. In addition, an optional restrictive action can be used to block the endpoint if the threat is Critical or High. This action is disabled by default.

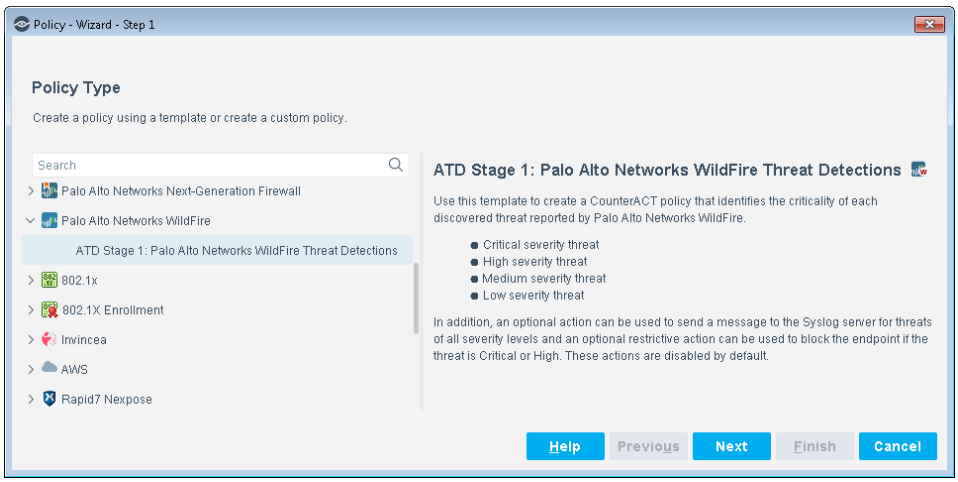
See Advanced Threat Detection with the IOC Scanner Plugin for information about threat detection and response stages. The IOC Scanner Plugin provides ATD Stage 2 and ATD Stage 3 policy templates that control when IOC Scanner endpoint scans are triggered and how scan results are interpreted. These policy templates should be used after you create a policy using the *ATD Stage 1: Palo Alto Networks WildFire Threat Detections* template.

Run the Template

This section describes how to create a policy from the policy template.

To run the 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 WildFire** folder and select **ATD Stage 1: Palo Alto Networks WildFire Threat Detections**. The template pane opens.

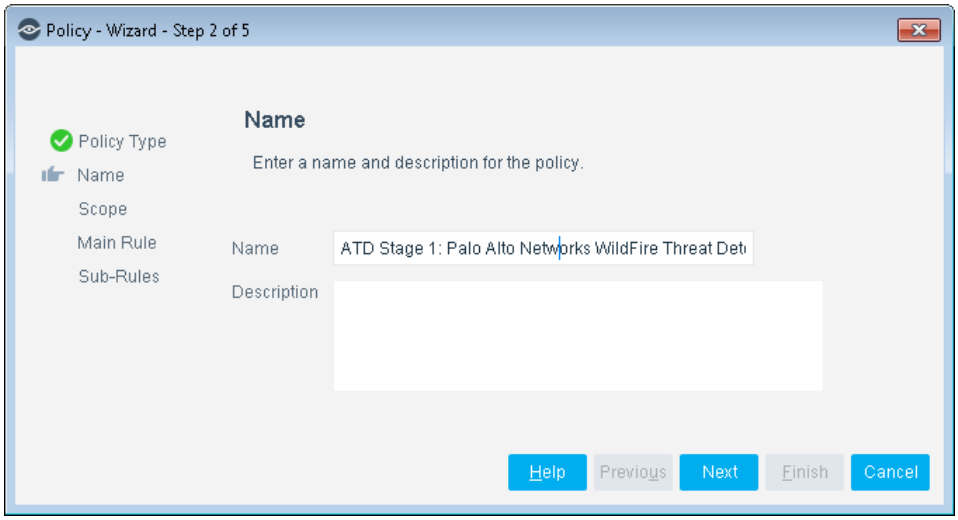


4. Select **Next.** The **Name** page opens.

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.

1. Define a unique name for the policy you are creating based on this template, and enter a description.



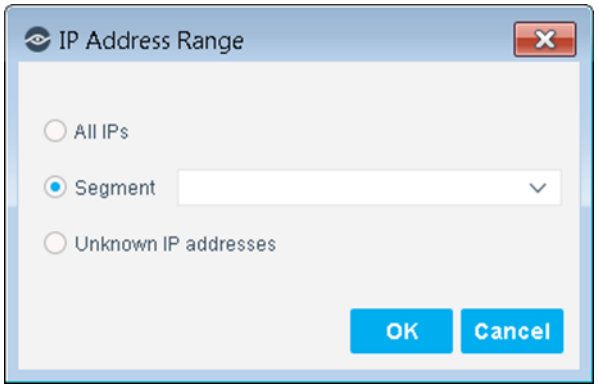
Naming Tips

- 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.

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

Define Which Hosts Will Be Inspected - Policy Scope

3. Use The IP Address Range dialog box to define which endpoints are inspected.



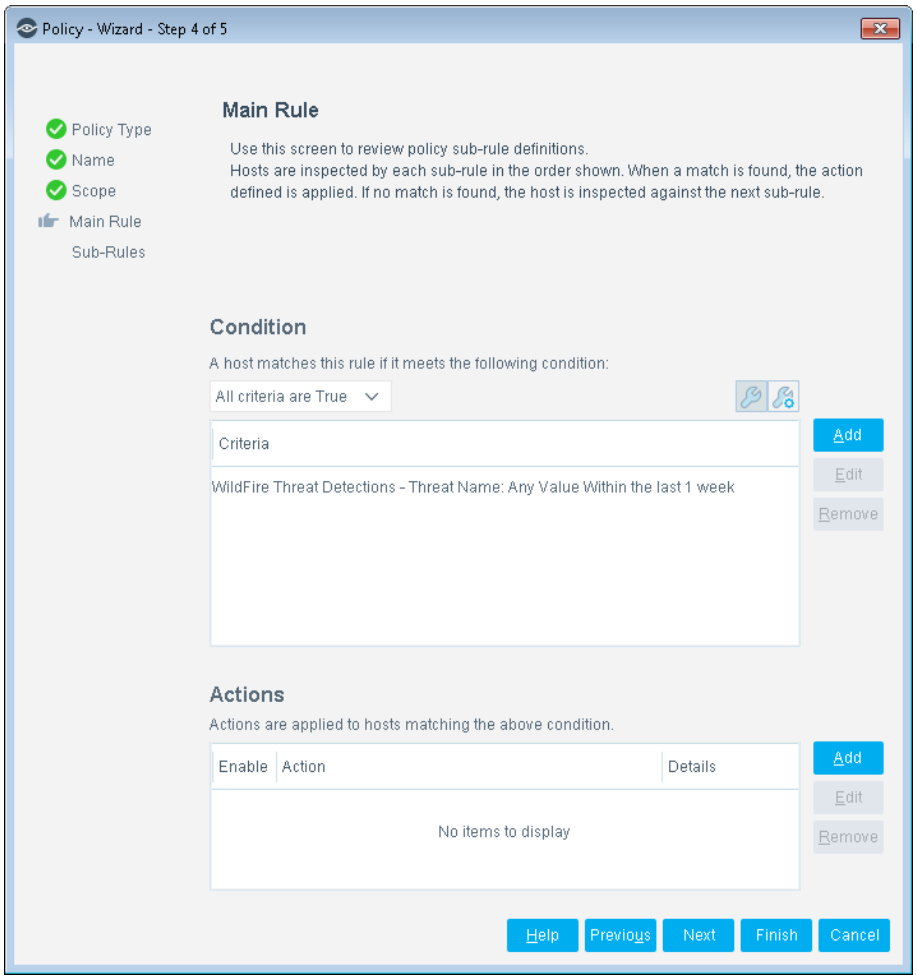
The following options are available:

- **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.

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

Main Rule

The main rule of this policy identifies any threat detected by the Palo Alto Networks WildFire server within the last week.



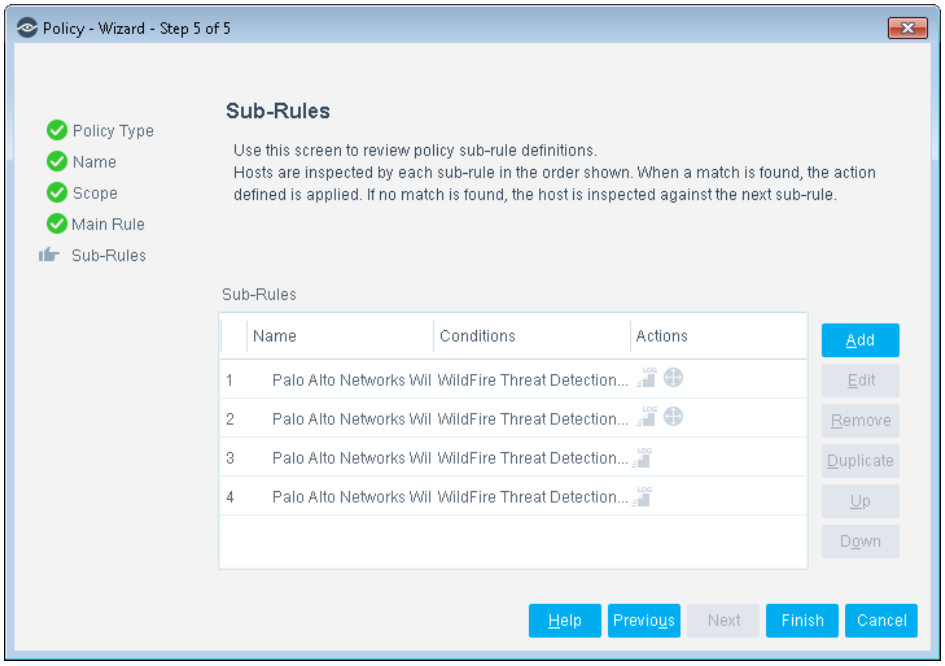
6. Select **Next** to add sub-rules to the policy, or select **Finish** to create the policy.

Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy*.

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. The sub-rules of this policy detect endpoints on which WildFire detected a threat severity of Critical, High, Medium or Low. An optional action can be used to send a message to the syslog server for threats of all severity levels and an optional restrictive action can be used to block the endpoint if the threat is Critical or High. These actions are disabled by default.



7. Select **Finish** to create the policy.
8. On the CounterACT Console, select **Apply** to save the policy.

Create Custom Palo Alto Networks WildFire Policies

CounterACT policies are powerful tools used for automated endpoint access control and management. You may need to create a custom policy to deal with issues not covered in the Palo Alto Networks WildFire policy template.

Policies and Rules, Conditions and Actions

CounterACT policies contain a series of rules. Each rule includes:

- Conditions based on host property values. CounterACT detects endpoints with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.
- Actions can be applied to endpoints that match the conditions of the rule.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with Palo Alto Networks WildFire related properties to create the custom policies. These items are available when you install the module.

You can also use the *Scan and Remediate Known IOCs* action and *Advanced Threat Detection* properties to create custom policies that:

- Scan potentially compromised Windows endpoints for IOCs reported by the Palo Alto Networks WildFire Module.
- Remediate infected endpoints.

These items are available when you install the IOC Scanner Plugin.

To create a custom policy:

1. In the CounterACT Console, select the **Policy** tab. The Policy Manager opens.
2. Select **Add** to create a policy, or select **Help** for more information about working with policies.

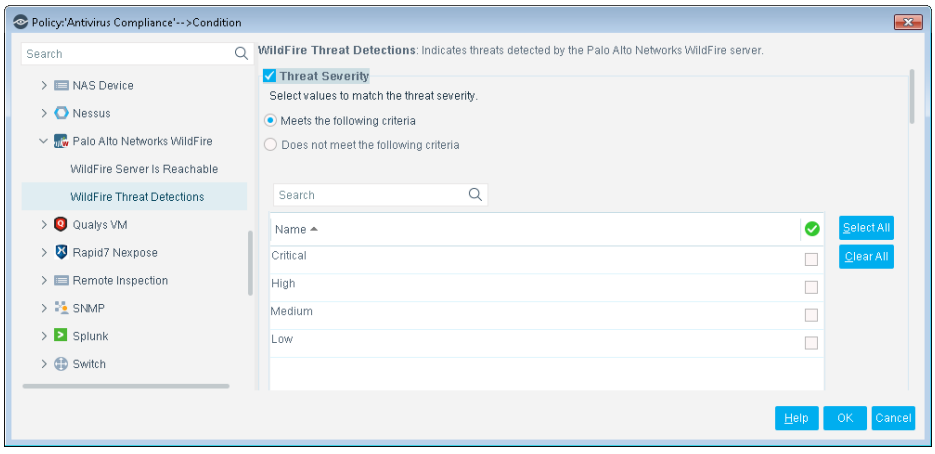
Palo Alto Networks WildFire – Policy Properties

This section describes the properties that are available when you install the Palo Alto Networks WildFire Module.

- WildFire Threat Detections
- WildFire Server Is Reachable

WildFire Threat Detections

Use the *WildFire Threat Detections* property in CounterACT policies to detect threats reported by Palo Alto Networks WildFire. For example, create a policy that detects if WildFire has detected a Critical severity threat, and trigger remediation when an endpoint meets this condition.

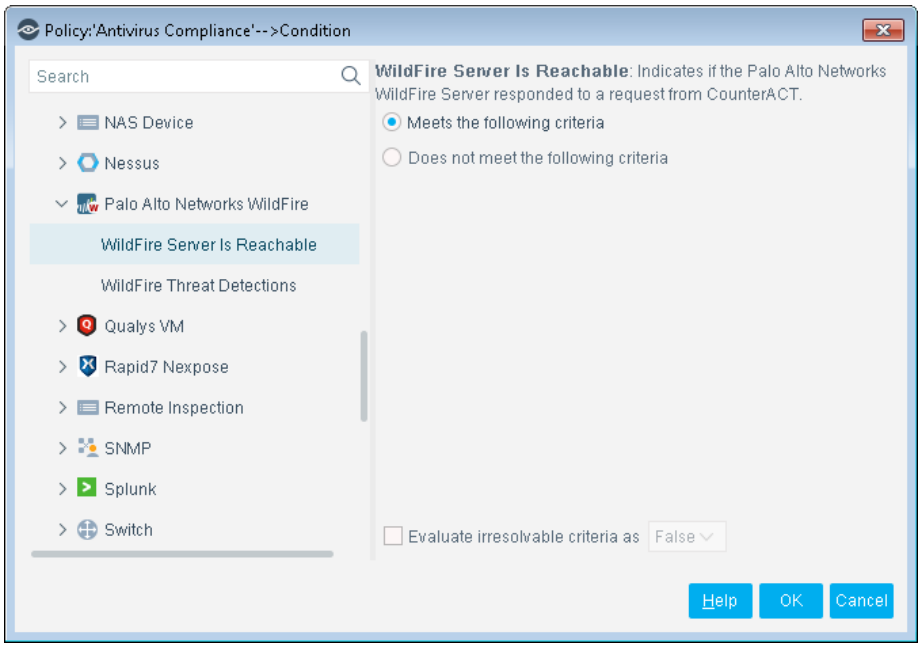


To access Palo Alto Networks WildFire properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the Palo Alto Networks WildFire folder in the Properties tree, and select **WildFire Threat Detections**. The following information is available:
   - Threat Severity
   - Threat Name
   - Threat File Name
   - Threat File Hash
   - Threat Hash Type
   - Date Reported

WildFire Server Is Reachable

Use the *WildFire Server Is Reachable* property in CounterACT policies to detect that the Palo Alto Networks WildFire server responded to a request from CounterACT.



To access Palo Alto Networks properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the Palo Alto Networks WildFire folder in the Properties tree, and select **WildFire Server Is Reachable**.

Display Asset Inventory Data

Use the CounterACT Asset Inventory to view a real-time display of threats detected by Palo Alto Networks WildFire.

The Asset Inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoints that have been detected with specific threats. For example, identify multiple endpoints detected with the same threat and analyze any shared endpoint characteristics that may be useful for determining how to handle the endpoints.
- Easily track Palo Alto Networks WildFire threat detection activity.
- Incorporate asset inventory detections into policies.

To access the Asset Inventory:

1. Select the **Asset Inventory** icon from the Console toolbar.
2. Navigate to **WildFire Threat Detections**.

The following information, based on the WildFire Threat Detections property, is available:

- Threat Severity
- Threat Name
- Threat File Name
- Threat File Hash
- Threat Hash Type
- Date Reported
- Last Update

Refer to *Working in the Console>Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console Online Help for information about working with the CounterACT Asset Inventory.

Core Extension Module Information

The PAN WildFire Module is installed with the CounterACT Core Extensions Module.

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

Advanced Tools Plugin	DNS Query Extension Plugin	NetFlow Plugin
CEF Plugin	External Classifier Plugin	Reports Plugin
Device Classification Engine	Flow Analyzer Plugin	Syslog Plugin
DHCP Classifier Plugin	IOC Scanner Plugin	Technical Support Plugin
DNS Client Plugin	IoT Posture Assessment Engine	Web GUI Plugin
DNS Enforce Plugin	NBT Scanner Plugin	

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are installed and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

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**.

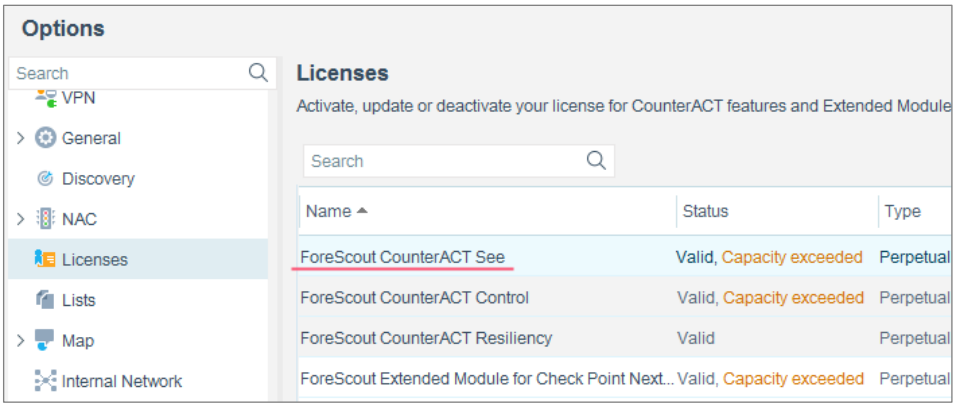
Documentation Portal

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

2018-04-15 17:23