



ForeScout

eyeExtend for Palo Alto Networks Wildfire

Configuration Guide

Version 2.2.2



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

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

2020-02-18 10:56

Table of Contents

About the Palo Alto Networks WildFire Integration.....	4
Advanced Threat Detection with the IOC Scanner Plugin	4
Use Cases	5
Additional Palo Alto Networks Documentation	5
About This Module.....	6
How It Works.....	7
What to Do.....	7
Requirements.....	8
Forescout Requirements	8
Forescout eyeExtend (Extended Module) Licensing Requirements.....	8
Per-Appliance Licensing Mode	9
Flexx Licensing Mode	10
More License Information	11
Palo Alto Networks Requirements	11
Configure the Palo Alto Networks Firewall	11
Configure the WildFire Module.....	11
Configure Communication with the Forescout Platform.....	12
Configure Communication with the Firewall.....	12
Configure Communication with Panorama.....	14
Install the Module	16
Configure the Module	16
Configure WildFire Servers	17
Test the WildFire Servers	21
Configure Firewall Servers.....	22
Create Palo Alto Networks WildFire Policies Using Templates.....	24
How Endpoints Are Detected and Handled	28
Create Custom Palo Alto Networks WildFire Policies	29
Palo Alto Networks WildFire – Policy Properties	29
WildFire Threat Detections.....	29
WildFire Server Is Reachable	30
Display Asset Inventory Data	31
Core Extension Module Information	32
Additional Forescout Documentation.....	32
Documentation Downloads	32
Documentation Portal	33
Forescout Help Tools.....	33

About the Palo Alto Networks WildFire Integration

Forescout eyeExtend for Palo Alto Networks® Wildfire, together with the IOC Scanner Plugin, integrates the Forescout platform 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 the Forescout platform to multiply the benefits of working with an Advanced Threat Detection product.

Forescout eyeExtend for Palo Alto Networks Wildfire enables the Forescout platform and Palo Alto Networks Wildfire to work together to find indicators of compromise (IOCs) quickly, detect advanced threats, contain infected endpoints, and disrupt the cyber kill chain, thus preventing further lateral threat propagation and data exfiltration. This helps the security team prevent, detect, analyze, and respond to advanced attacks.

Advanced Threat Detection with the IOC Scanner Plugin

Forescout eyeExtend for Palo Alto Networks Wildfire works with the IOC Scanner Plugin, Forescout's platform 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 the Forescout platform 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 the Forescout platform, evaluate the likelihood of compromise, and apply appropriate actions to endpoints.

Threat detection and response is implemented in the following stages:

- **ATD Stage 1 (Forescout eyeExtend for Palo Alto Networks Wildfire): 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 Forescout platform 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 the Forescout platform'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 *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide*.

Use Cases

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

- Receive alerts from Palo Alto Networks on threats detected and immediately perform restrictive actions on the endpoints on which they were detected.
- Scan all Windows endpoints for IOCs reported to the Forescout platform by Palo Alto Networks Wildfire to identify threats and perform actions on potentially infected endpoints. For example, use Forescout platform 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, for example, by sending an email to corporate security teams with details about which threats were detected on which endpoints.

For detailed information about this use case, refer to the section about use cases in the *Forescout Core Extensions Module: 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

Forescout eyeExtend for Palo Alto Networks Wildfire, together with the IOC Scanner Plugin, lets you integrate the Forescout platform with Palo Alto Networks Wildfire so that you can:

- Use the [Create Palo Alto Networks WildFire Policies Using Templates](#) 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 Forescout 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 *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide* for details.

IOC Scanner

The IOC Scanner Plugin automatically collects threats and their indicators of compromise (IOCs) reported by installed plugins.

[IOC Repository](#) [Threat Exceptions](#)

Manage the centralized IOC repository of threats that were reported to CounterACT by Advanced Threat Detection (ATD) systems or that were added manually.

Search

Date Reported	Reported By	Threat Name	File Name	File Size (bytes)	File Hash	Hash Type	Threat Severity	Operating System	
7/2/17 11:01:20 AM	Palo Alto WildFire	Trojan Kelhos	newbos2.exe	767,488	448009c290d00fca	MD5	High	Win	Add
7/2/17 11:05:11 AM	Palo Alto WildFire	Trojan Kelhos	newbos2.exe	767,488	448009c290d00fca	MD5	High	Win	Edit
7/2/17 11:07:00 AM	Palo Alto WildFire	Malware.archive	newbos2.exe.zip	1	448009c290d00fca	MD5	High	Win	Remove
7/2/17 11:08:00 AM	Palo Alto WildFire	Virus Parite.MVX	nc—15-49.exe	176,128	448009c290d00fca	MD5	High	Win	IOCs
7/2/17 11:09:24 AM	Palo Alto WildFire	Virus Parite.MVX	nc—15-49.exe	176,128	448009c290d00fca	MD5	High	Win	
7/2/17 12:27:14 PM	Palo Alto WildFire	Test.Backdoor	bad.txt	1	448009c290d00fca	-None-	Critical	Win	

6 items (0 selected)

Threats of Medium severity and lower are automatically deleted 14 days after being reported. All threats are automatically deleted 30 days after being reported.

[Apply](#) [Undo](#)

- Use the Forescout platform 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 the Forescout platform 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 the Forescout platform 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. The Forescout platform detects .dll or .exe Portable Executable file types only.
 - File Names
 - Registry Keys and Values
 - Service Names
 - DNS Queries
 - Command and Control (CnC) URLs

The Forescout platform adds the data to its IOC repository and resolves the data as Forescout 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. The Forescout platform can use this information to detect the same threat on other endpoints. For example, the Forescout platform can scan endpoints not protected by Palo Alto Networks WildFire, detect IOCs used during a threat infection phase, and trigger a threat remediation action.

Refer to the *Forescout Core Extensions Module: IOC Scanner Plugin Configuration Guide* for details.

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See [Requirements](#).
2. [Configure the Palo Alto Networks Firewall](#).
3. [Install the Module](#).
4. [Configure the Module](#).

5. (Optional) [Create Palo Alto Networks WildFire Policies Using Template.](#)
6. (Optional) [Create Custom Palo Alto Networks WildFire Policies.](#)

Requirements

Verify that the following requirements are met:

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

Forescout Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.1.
- Core Extensions Module version 1.1, with the following components running (see [Core Extension Module Information](#)):
 - Syslog Plugin
 - IOC Scanner Plugin
- A module license for Forescout eyeExtend for Palo Alto Networks Wildfire. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).

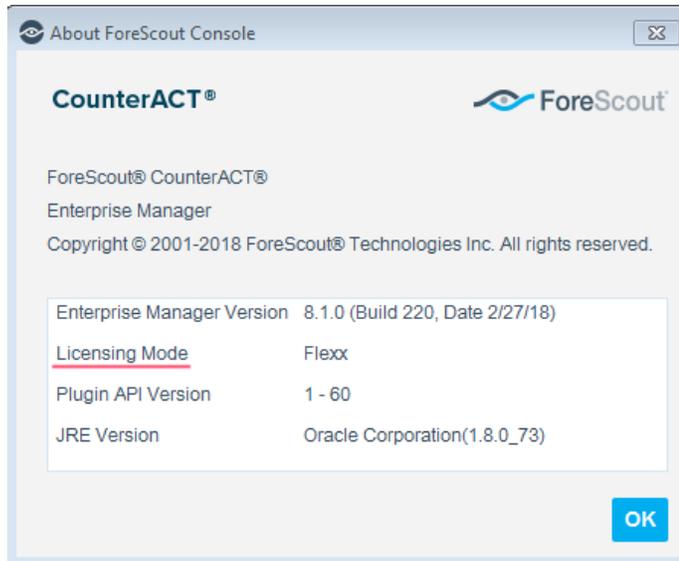
Forescout eyeExtend (Extended Module) Licensing Requirements

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

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

To identify your licensing mode:

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



Per-Appliance Licensing Mode

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

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

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

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

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

Requesting a License

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

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



To view the number of currently detected devices:

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



Flexx Licensing Mode

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

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

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

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

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

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

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

Palo Alto Networks 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-premises 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:

- [Configure the WildFire Module](#)
- [Configure Communication with the Forescout Platform](#)

Configure the WildFire Module

Configure Forescout eyeExtend for Palo Alto Networks Wildfire as follows:

- Set 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.

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

Configure Communication with the Forescout Platform

In the Palo Alto Networks Firewall UI, you need to define each connecting CounterACT device as a syslog server that receives Palo Alto Networks WildFire syslog messages.

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

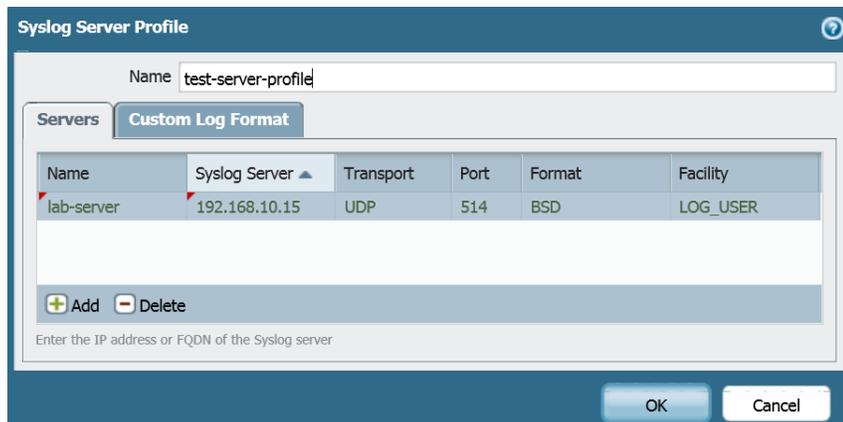
You can configure this communication per firewall or via Panorama. Panorama provides centralized monitoring and management of multiple Palo Alto Networks firewalls.

- [Configure Communication with the Firewall](#)
- [Configure Communication with Panorama](#)

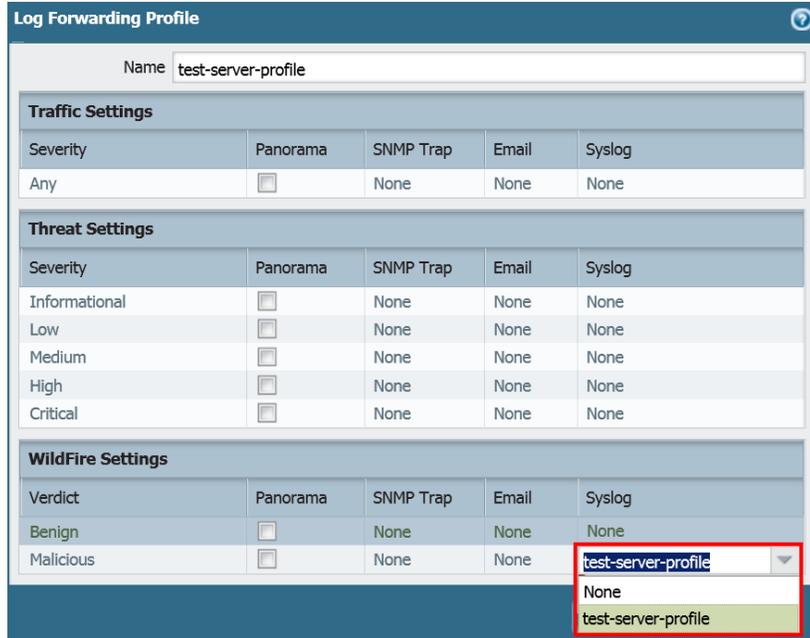
Configure Communication with the Firewall

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**.



2. 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.
3. Create a Log Forwarding Profile and select the threat logs to be forwarded to the syslog server:
 - a. Select **Objects > Log forwarding > Add**.



- 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 resemble the following:

<input type="checkbox"/>	Name	Location	Log Type	Severity	To Panorama	SNMP Trap	Email	Syslog
<input checked="" type="checkbox"/>	test-server-profile		Threat					
			WildFire	malicious				test-server-profile
			Traffic					

- 4. 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**.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab active. The 'Action Setting' section has 'Allow' selected. The 'Profile Setting' section has 'Profile Type' set to 'Profiles' and 'File Blocking' set to 'WildFire for CounterACT'. The 'Log Setting' section has 'Log at Session End' checked and 'Log Forwarding' set to 'test-server-profile'. The 'Other Settings' section includes 'Schedule' (None), 'QoS Marking' (None), and 'Disable Server Response Inspection' (unchecked). 'OK' and 'Cancel' buttons are at the bottom right.

d. Select the following:

In the Log Setting area, select the *Log Forwarding* profile created in step [3](#) 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 drop-down menu in addition to the profiles listed above. The WildFire Analysis option is displayed in the Profile Setting area.*

e. Select **OK**.

Configure Communication with 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**.

Syslog Server Profile

Name: test-server-profile

Servers Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
lab-server	192.168.10.15	UDP	514	BSD	LOG_USER

+ Add - Delete

Enter the IP address or FQDN of the Syslog server

OK Cancel

- 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**.

Collector Group

General Monitoring Device Log Forwarding Collector Log Forwarding

Name: test-collector-group

Log Storage Total: 0 MB, Free: 0 MB

Min Retention Period (days): [1 - 2000]

Enable log redundancy across collectors

OK Cancel

- b. In the General tab, enter a name.
 - c. Select **Collector Log Forwarding > WildFire**.

Collector Group

General Monitoring Device Log Forwarding Collector Log Forwarding

System Config HIP Match Traffic Threat WildFire Correlation

Verdict	SNMP Trap	Email	Syslog
Benign			
Grayware			
Malicious			test-server-profile

OK Cancel

- 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](#) - **Flexx Licensing Mode**

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

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

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

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

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

 *Some components are not automatically started following installation.*

Configure the Module

After you install Forescout eyeExtend for Palo Alto Networks Wildfire, configure the module for the Forescout platform to communicate with the WildFire service.

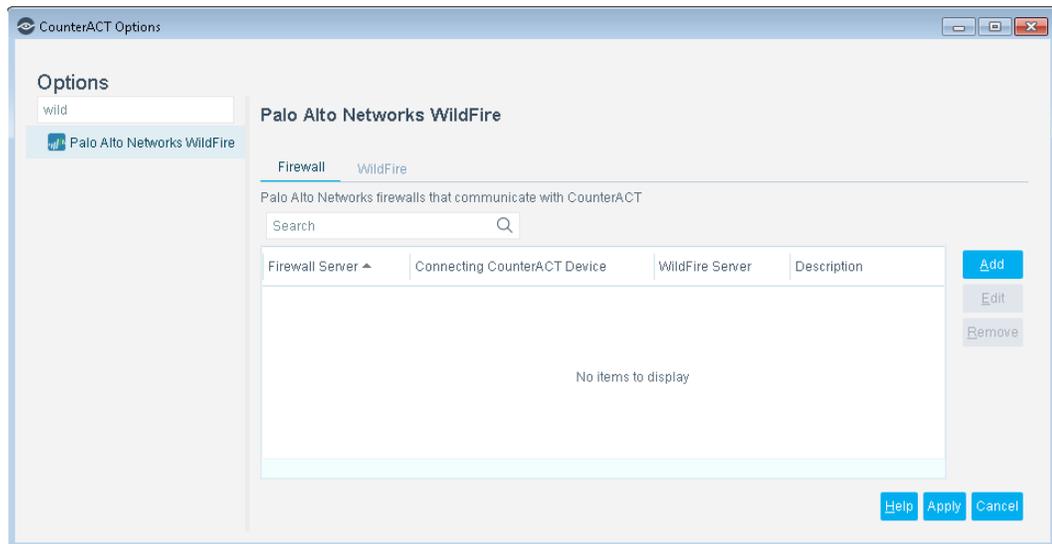
- Define each WildFire server and its login credentials. See [Configure WildFire Servers](#).
- Define each Firewall server, including the name of a defined WildFire server and the CounterACT device it communicates with. See [Configure Firewall Servers](#).

Configure WildFire Servers

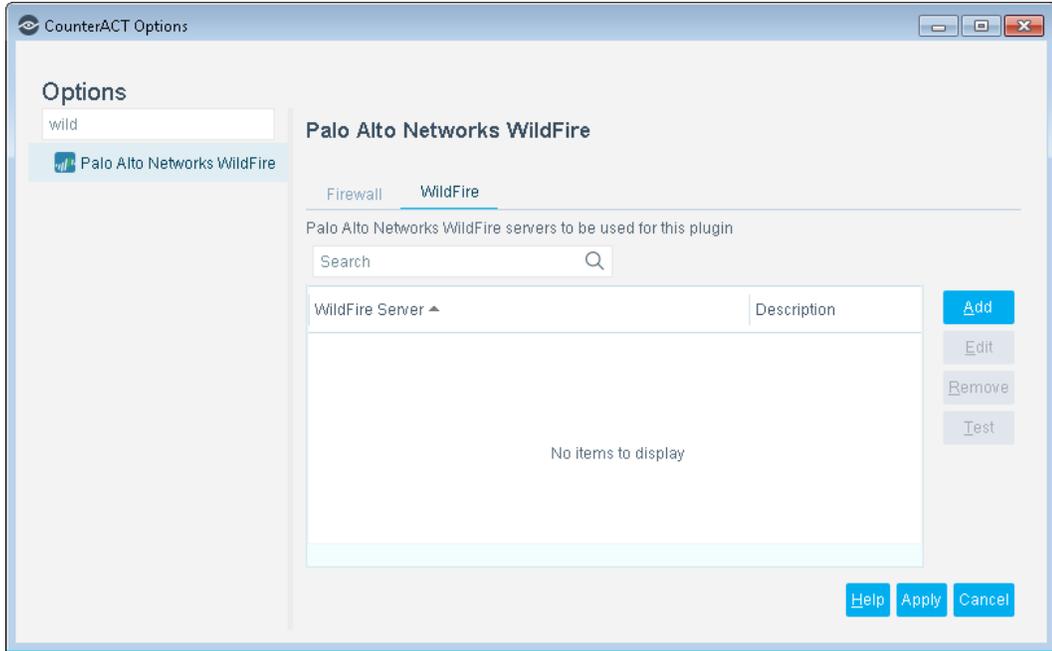
WildFire servers provide IOC details of the threats detected by Palo Alto Networks WildFire. Define each WildFire server and its login credentials.

To define WildFire servers:

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



4. Select the Wildfire tab.



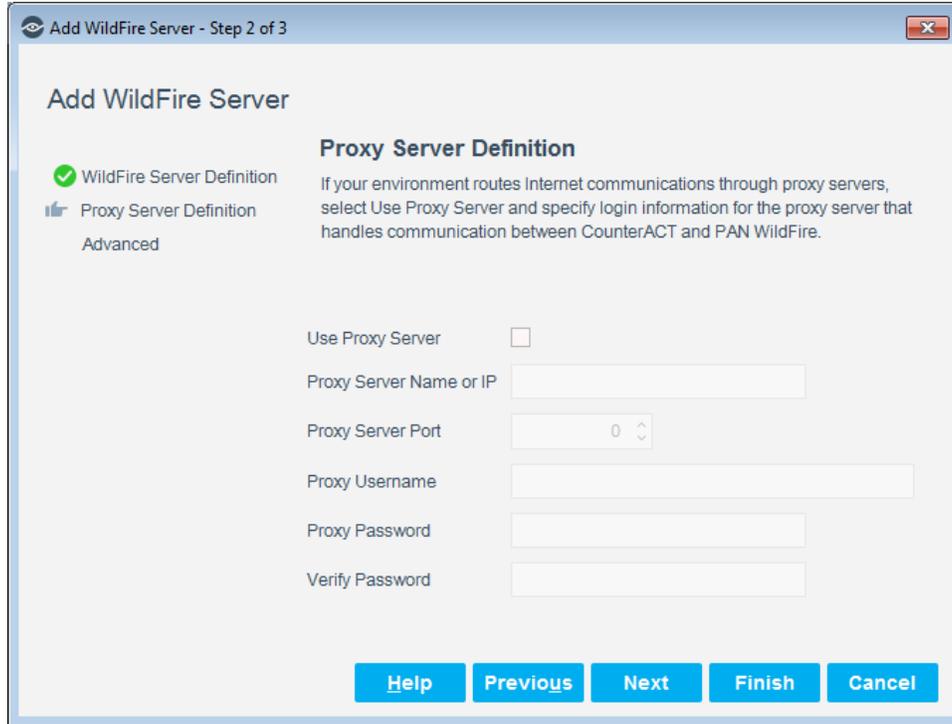
- 5. Select **Add** to define a Palo Alto Networks WildFire server to provide IOC details of reported threats to the Forescout platform.



6. Configure the following settings:

Use PAN WildFire Public Cloud	<p>Select this option to automatically display the server name in the WildFire Server Name or IP field. Determines if WildFire is in a public cloud.</p> <p><i>Verify that the Connecting CounterACT Device has access to the public cloud. The Forescout platform uses port 443 to communicate with WildFire. The Firewall and the WildFire public cloud use ports 443 and 10443 to communicate with each other.</i></p>
WildFire Server Name or IP	<p>Enter the server name, a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the WildFire server.</p>
WildFire Server API Access Key	<p>Enter the login credentials for the WildFire server. Contact Palo Alto Networks for information on how to obtain this key.</p>
Verify Key	<p>Retype the key to confirm it.</p>
Validate Server Certificate	<p>Select this option to validate the identity of the third-party server before establishing a connection when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>

7. Select **Next**.



8. Configure the following settings:

Use Proxy Server	Select this option to use a proxy server to communicate with PAN WildFire.
Proxy Server Name or IP	Enter the proxy server name, a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the proxy server.
Proxy Server Port	Enter the port used to communicate with the proxy server.
Proxy Username	Enter the login name for an authorized account defined on the proxy server, if required.
Proxy Password	Enter the password for the above user, if required.
Verify Password	Retype the password to confirm it.

9. Select **Next**.



10.(Optional) In the **Description** field, enter a textual description of the WildFire server. Select **Finish**.

11.Select **Apply**.

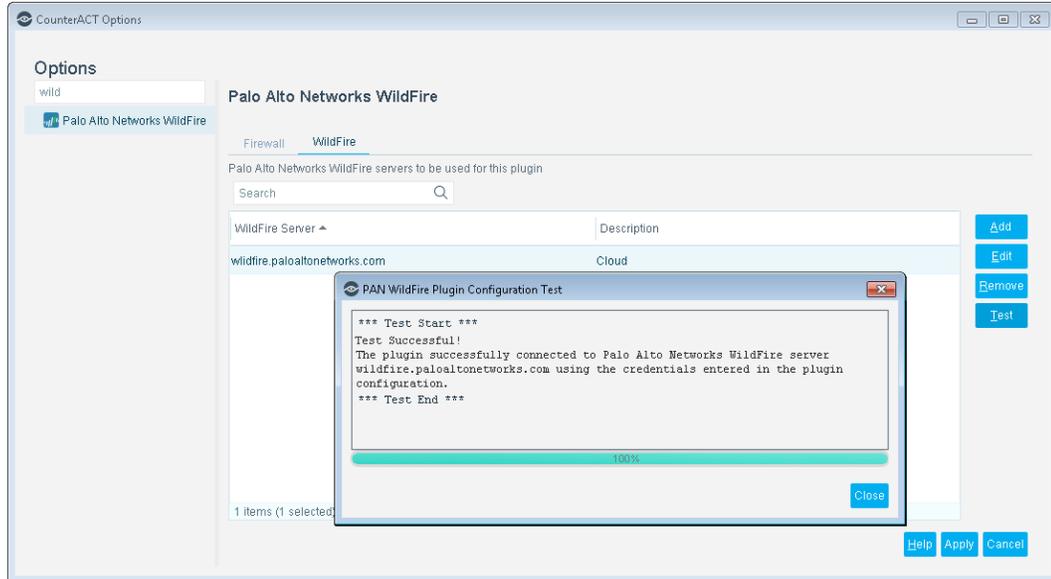
The best practice is to perform a test after setting up a connection. See [Test the WildFire Servers](#).

Test the WildFire Servers

Test each WildFire server configuration to ensure that Forescout eyeExtend for Palo Alto Networks Wildfire 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:

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

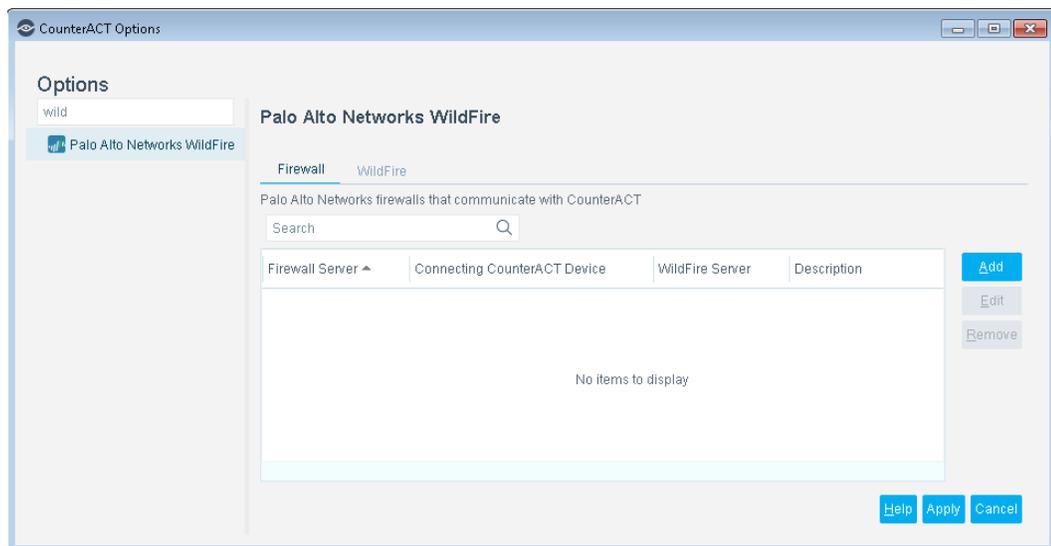


Configure Firewall Servers

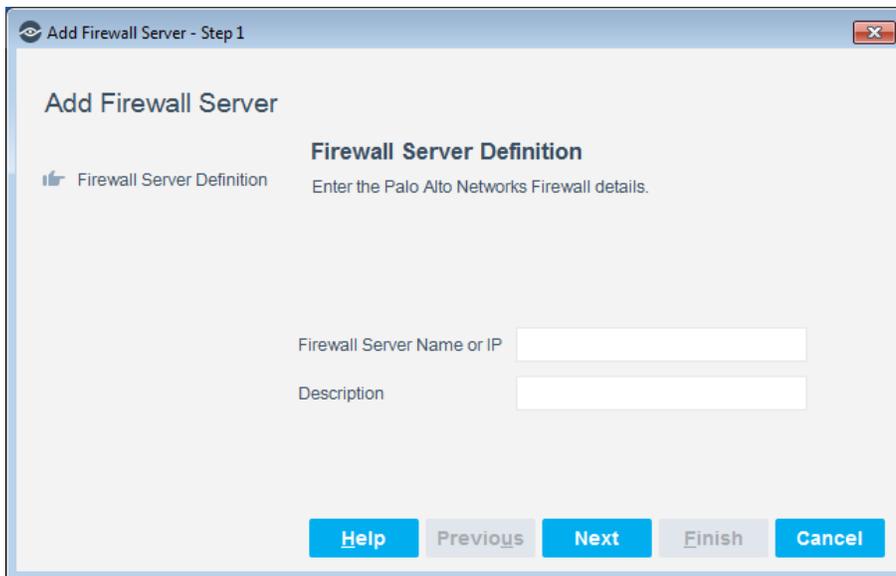
The Firewall sends the initial alert of detected threats to the Forescout platform. Define Firewall server information, along with information about the configured WildFire server and the CounterACT device that communicates with the WildFire server.

To define Firewall servers:

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



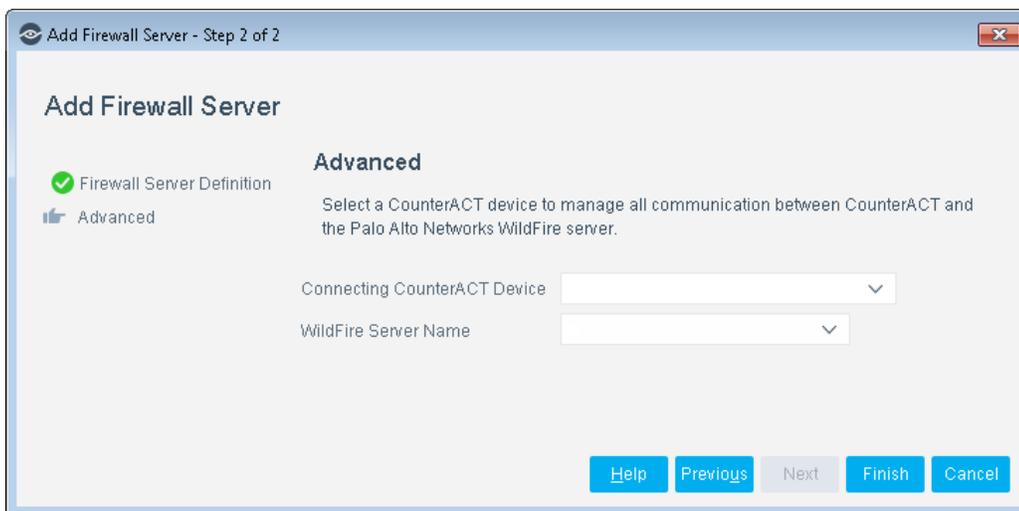
2. Select **Add** to define a Palo Alto Networks Firewall server to communicate with the Forescout platform.



3. Configure the following settings:

Firewall Server Name or IP	Enter the server name, a Fully Qualified Domain Name (FQDN), or the IPv4 or IPv6 address of the Firewall server.
Description	(Optional) A textual description of the Firewall server.

4. Select **Next**.



5. Configure the following settings:

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 the Forescout Platform for details.
-------------------------------------	---

WildFire Server Name	WildFire server defined in the Configure WildFire Servers section.
-----------------------------	--

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

Create Palo Alto Networks WildFire Policies Using Templates

Forescout eyeExtend for Palo Alto Networks Wildfire provides the ATD Stage 1: Palo Alto Networks WildFire Threat Detections template, which you can use to handle threats in a Palo Alto Networks WildFire environment.

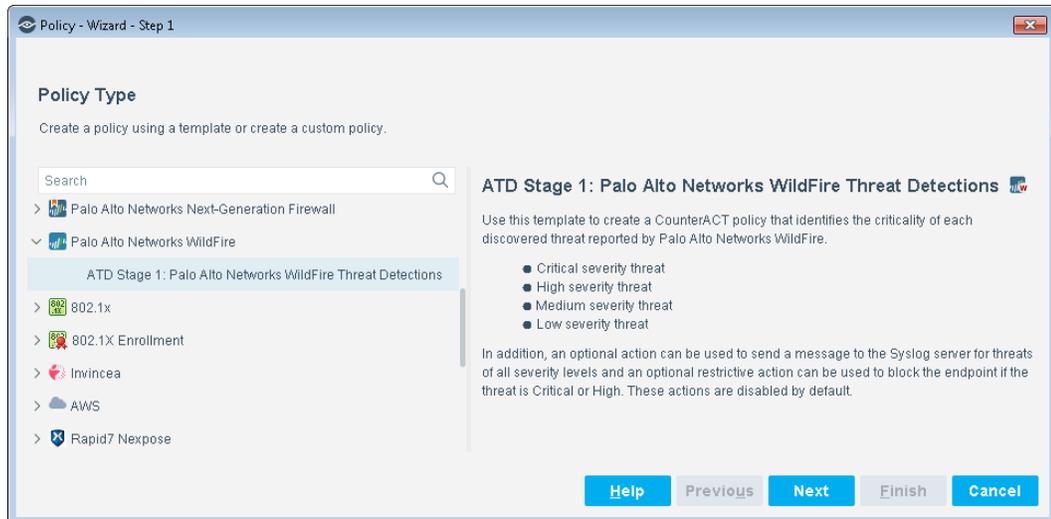
Use the ATD Stage 1: Palo Alto Networks WildFire Threat Detections policy to identify the criticality of each discovered threat reported by Palo Alto Networks WildFire and then send a message to the syslog server. In addition, an optional restrictive action can be used to block the endpoint if the threat 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.

 *It is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.*

To create an ATD Stage 1 policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Palo Alto Networks WildFire** folder and select **ATD Stage 1: Palo Alto Networks WildFire Threat Detections**.



4. Select **Next**.



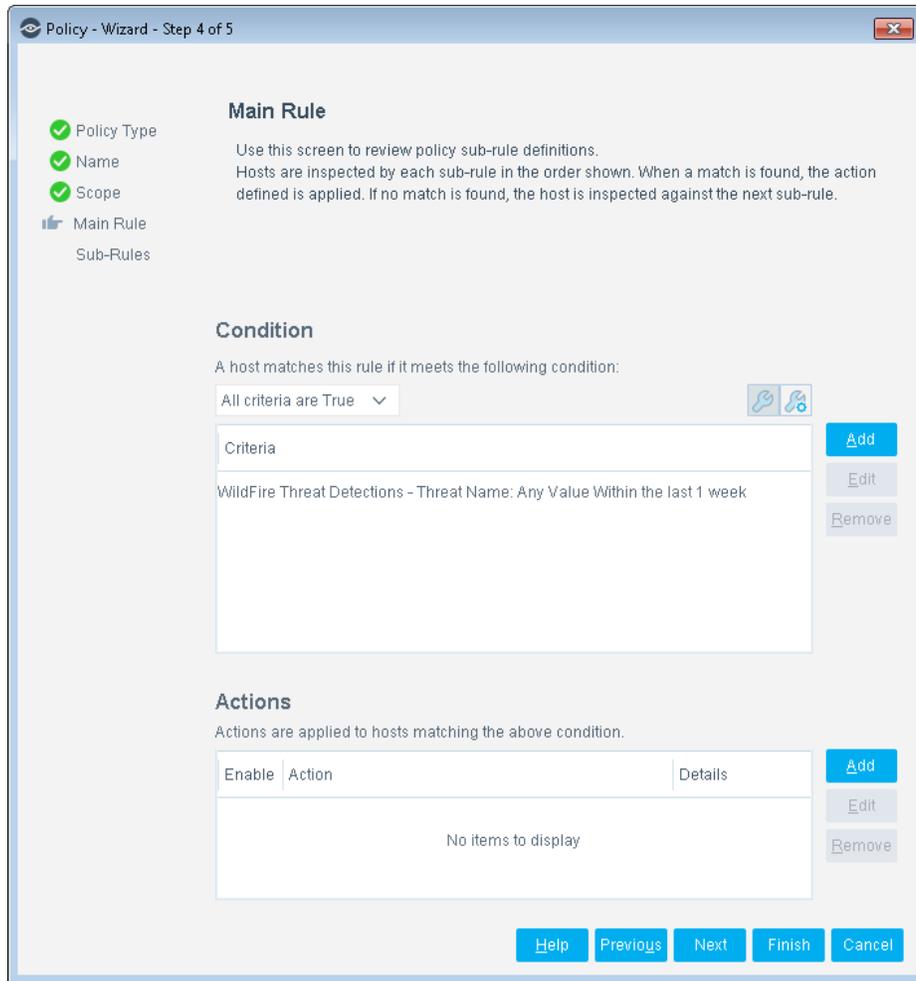
5. Define a unique name for the policy you are creating based on this template and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
 - Use a descriptive name that indicates what your policy is verifying, and which actions are taken.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports, and in other features. Precise names make working with policies and reports more efficient.*
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



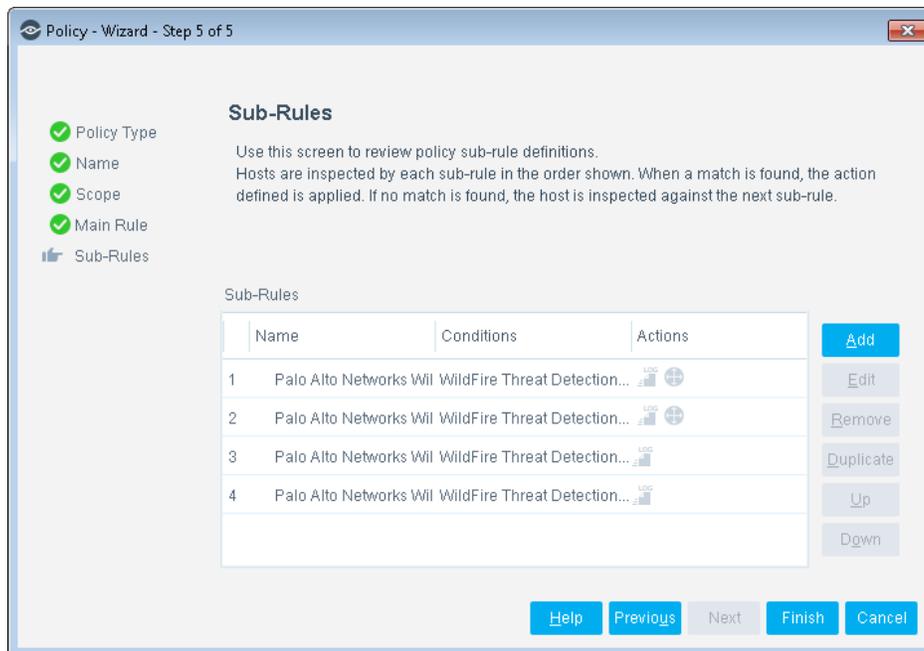
The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
- 8.** Select **OK**. The added range is displayed in the Scope pane.
 - 9.** Select **Next**.



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

10.Select **Next** to view or edit the Sub-rules pane.



11. The sub-rules of this policy detect threats based on their reported severity. For details, see [How Endpoints Are Detected and Handled](#).
12. In the Sub-Rules pane, select **Finish**.
13. In the Console, select **Apply** to save the policy.

How Endpoints Are Detected and Handled

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

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 let you 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.

Create Custom Palo Alto Networks WildFire Policies

Forescout platform 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

Forescout platform policies contain a series of rules. Each rule includes:

- Conditions based on host property values. The Forescout platform 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 Forescout 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 Forescout eyeExtend for Palo Alto Networks Wildfire.
- Remediate infected endpoints.

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

To create a custom policy:

1. In the Console, select **Policy**. 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 Forescout eyeExtend for Palo Alto Networks Wildfire.

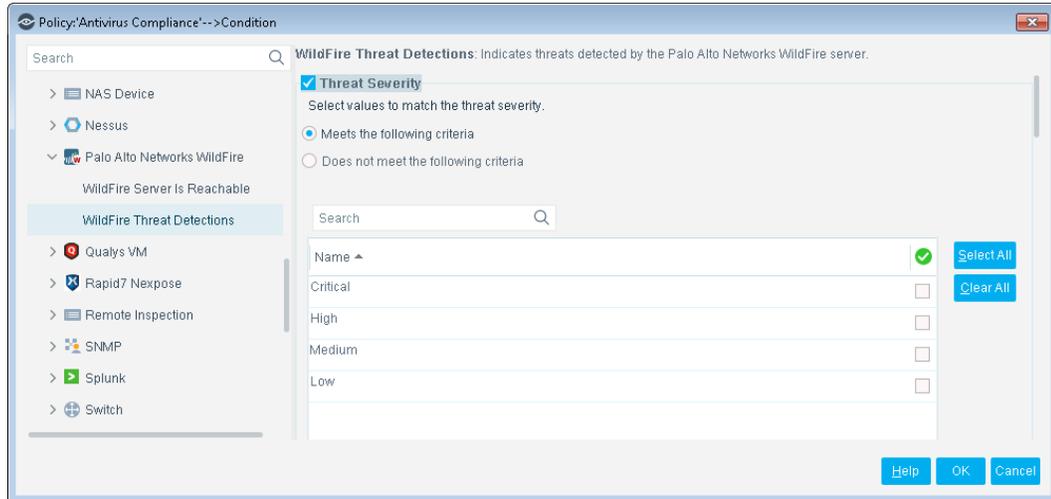
- [WildFire Threat Detections](#)
- [WildFire Server Is Reachable](#)

WildFire Threat Detections

Use the WildFire Threat Detections property in Forescout platform 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. Go 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**.

**3. The following information is available:**

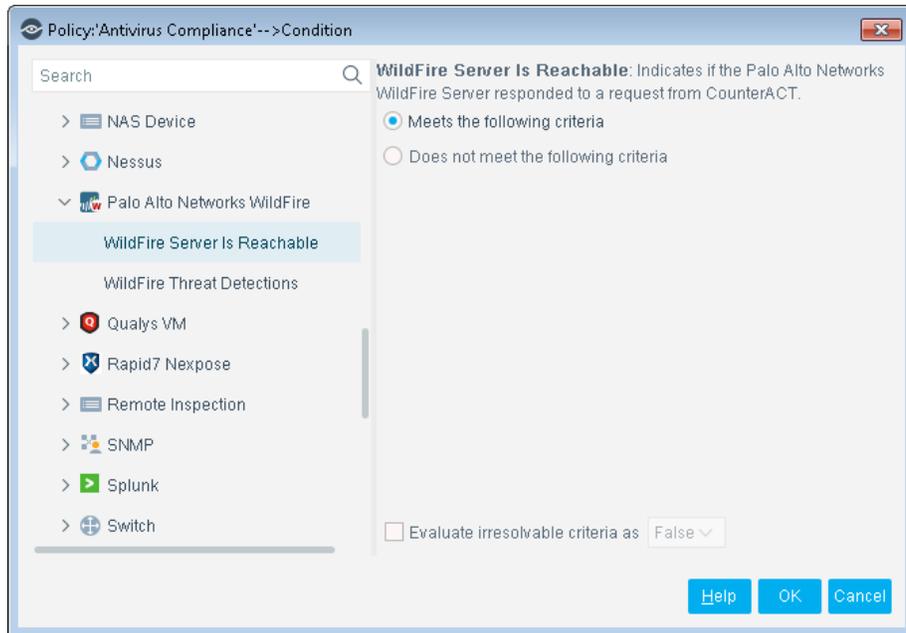
- Threat Severity
- Threat Name
- Threat File Name
- Threat File Hash
- Threat Hash Type
- Date Reported

WildFire Server Is Reachable

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

To access Palo Alto Networks properties:

1. Go 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 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. In the Console, select **Asset Inventory**.
2. Go 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 *Forescout Administration Guide* or the Console Online Help for information about working with the Asset Inventory.

Core Extension Module Information

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

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

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

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. Upgrading the Forescout version or performing a clean installation installs this module automatically.

Additional Forescout Documentation

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

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

Documentation Downloads

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

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

 Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

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

To access the Forescout Resources page:

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

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Portal

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

To access documentation on the Forescout Customer Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

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

Plugin Help Files

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

Online Documentation

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