

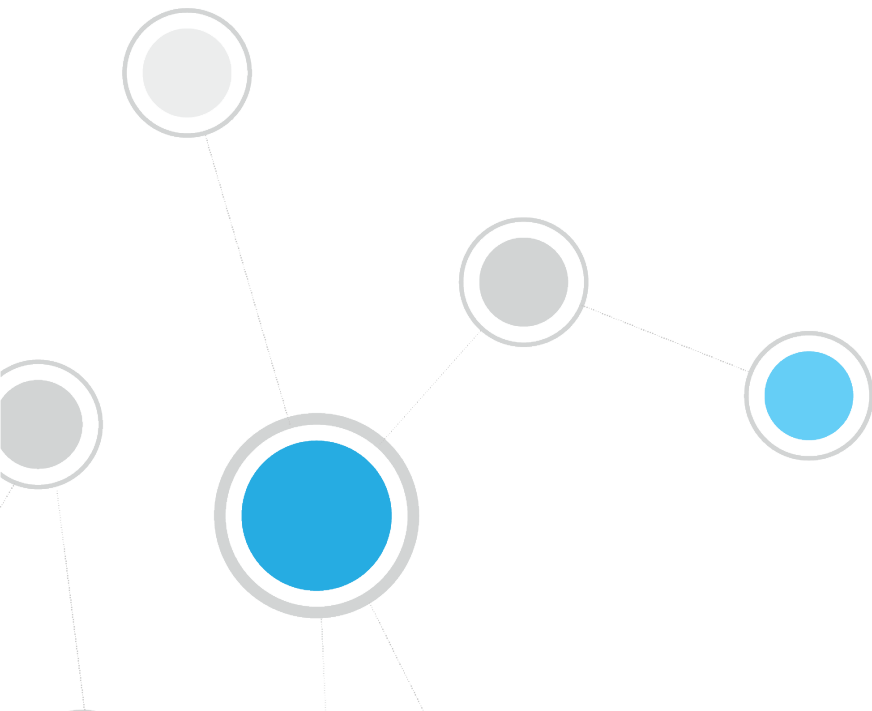


# ForeScout CounterACT<sup>®</sup>

## Prevent Network Attacks

How-to Guide

**Version 8.0**





## Table of Contents

<b>About Preventing Network Attacks .....</b>	<b>3</b>
<b>Prerequisites .....</b>	<b>3</b>
<b>Create and Apply a Threat Protection Policy.....</b>	<b>4</b>
<b>Evaluate Threats .....</b>	<b>7</b>
<b>Generate Reports .....</b>	<b>8</b>
<b>Additional CounterACT Documentation .....</b>	<b>9</b>
Documentation Downloads .....	9
Documentation Portal .....	10
CounterACT Help Tools.....	10




## About Preventing Network Attacks

ForeScout CounterACT<sup>®</sup> provides powerful tools that let you continuously track and control four common categories of threats to your organizational network:

- **Malicious Hosts:** Harmful network activity, such as a worm infection or malware propagation attempts.
- **ARP Spoofing:** Attempts to illegally gain access to your organizational network, modify the traffic, or stop the traffic altogether using the Address Resolution Protocol.
- **Impersonation:** Attempts to masquerade as a legitimate corporate device in order to gain access to your network.
- **Dual Homed:** De facto bridge connection to your organizational network, created by a host such as a rogue wireless access point.

Follow the step-by-step procedures in this guide to:

- Use a wizard-based CounterACT template to create a Threat Protection policy that detects threats to your network. Optional notification actions, disabled by default, can be used to inform users at the malicious endpoint, as well as the CounterACT administrator, that the endpoint is threatened.
- Review an extensive range of information about threats at hosts and about the users connected to them.
- Generate real-time and trend reports on threatening activity across your network.

 *This How-to guide provides basic configuration instructions designed for a quick setup. For more information on the extended configuration options, refer to the CounterACT Administration Guide.*

## Prerequisites

- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the CounterACT Administration Guide for details.



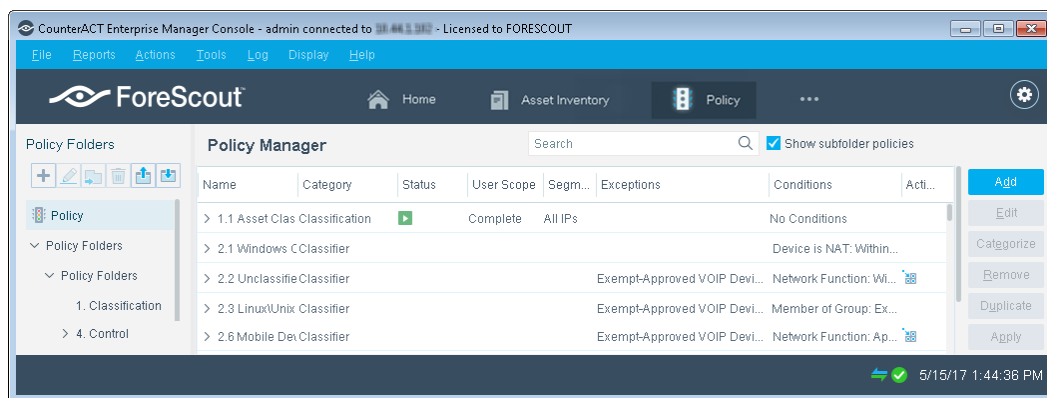
# Create and Apply a Threat Protection Policy

Follow these steps to detect threats to your network using a policy template.

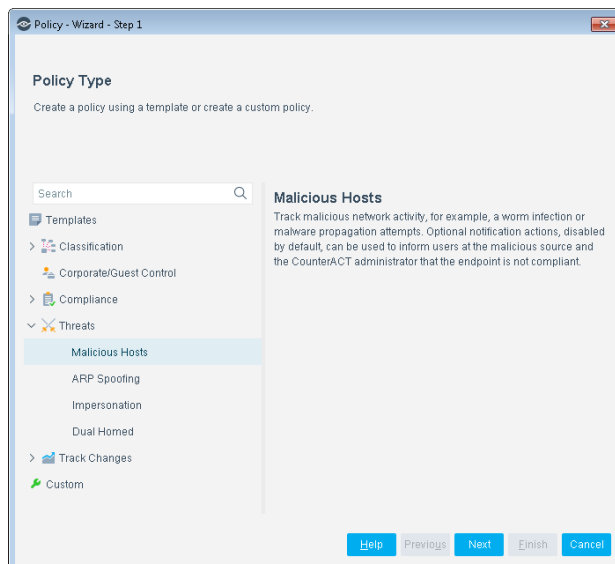
This guide discusses malicious hosts, but it also applies to ARP spoofing, impersonation and dual-homed hosts.

## 1 Select the Malicious Hosts Template

1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



3. In the Policy Manager pane select **Add**. The Policy Wizard opens, guiding you through policy creation.



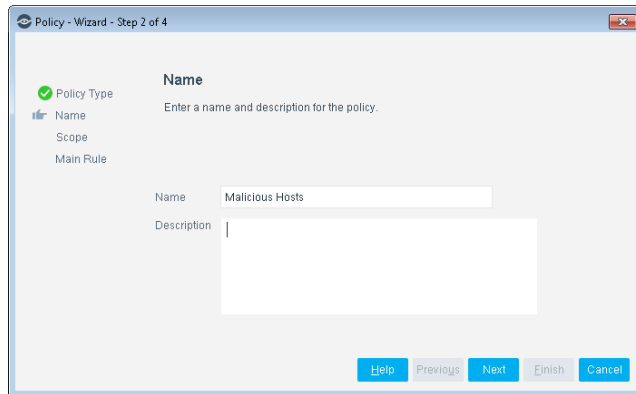
4. Under **Templates**, expand the **Threats** folder and select **Malicious Hosts**.



5. Select **Next**. The Policy Name pane opens.

## 2 Name the Policy

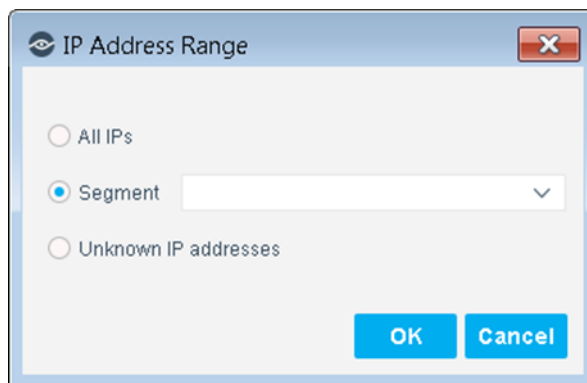
1. In the Name pane, a default policy name appears in the **Name** field.



2. Accept the default name or create a new name, and add a description.
3. Select **Next**. The Scope pane and the IP Address Range dialog box opens.

## 3 Choose the Hosts to Inspect

1. 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.  
Not applicable for this policy template.

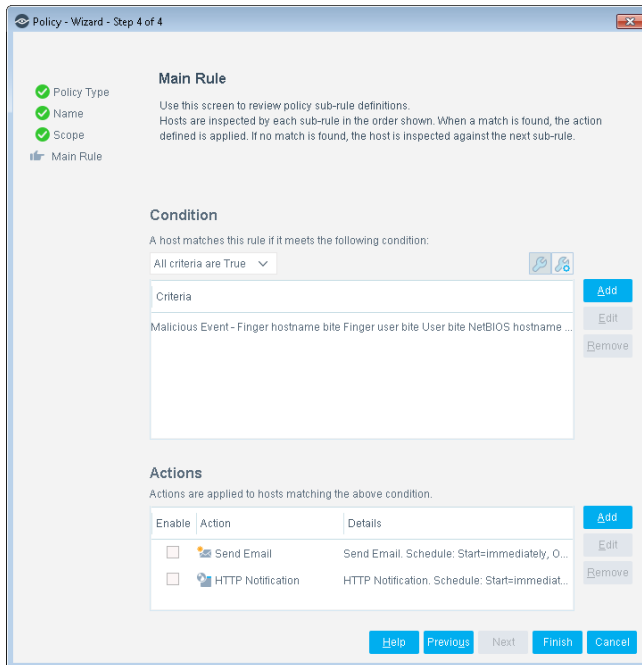


📄 Viewing or modifying the Internal Network is performed separately. Select **Tools>Options>Internal Network**.

2. Select **OK**. The added range appears in the Scope list.
3. Select **Next**. The Main Rule pane opens.

#### 4 Finish Policy Creation

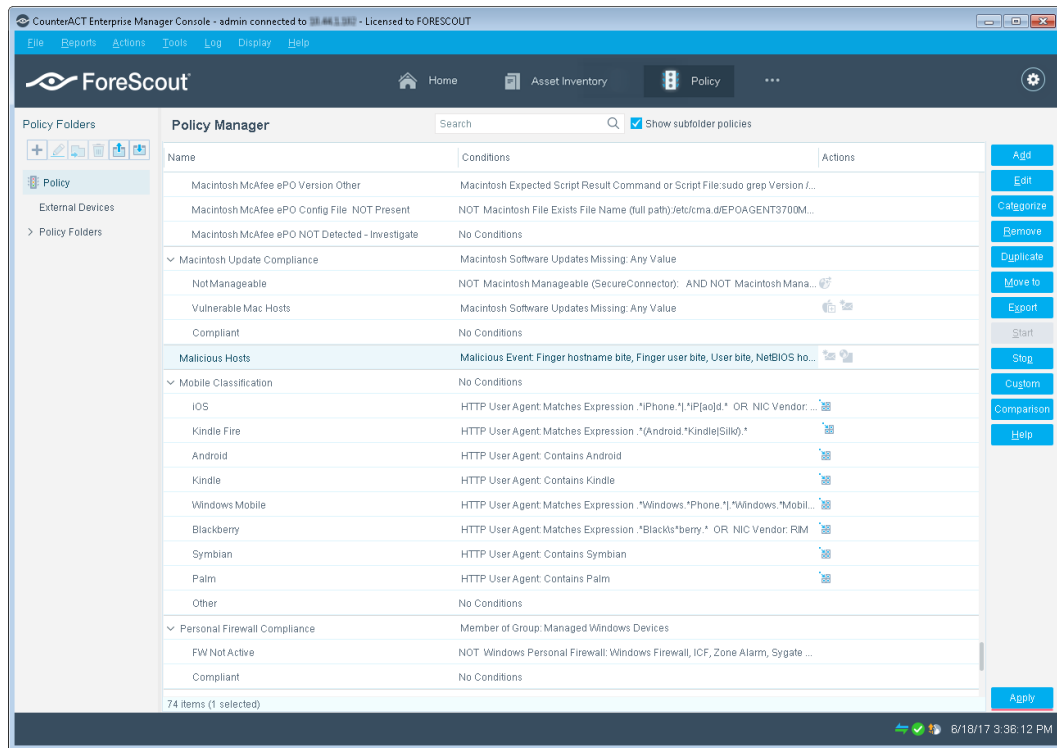
The policy main rules are displayed in the Main Rule pane. Rules instruct CounterACT how to detect hosts (Condition) and handle hosts (Actions). Optional notification actions, disabled by default, can be used to notify endpoint users or the CounterACT administrator that the endpoint is threatened. After you have run the policy and verified that results accurately reflect your network, you can remediate by enabling these actions.



1. Select **Finish**. The policy automatically appears highlighted in the Policy Manager, where it can be activated.

#### 5 Activate the Policy

1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, select the policy you created.



3. Select **Apply**. The policy is activated.

## Evaluate Threats

After activating the policy, you can view an extensive range of details about endpoints under threat of network attacks.

**To view details about endpoints and end users under threat of network attacks:**

1. On the Console toolbar select the Home tab.
2. In the Views pane, expand the **Policy** folder and scroll to the policy containing your Malicious Hosts policy.
3. In the Detections pane, select a host. Host information is displayed in the Details pane.




The screenshot displays the ForeScout CounterACT Enterprise Manager Console interface. The main window shows a table titled "Malicious Hosts" with 16 entries. The table columns are: Host, HostIP, Segment, Policy Malicious Hosts, MAC Address, Function, and Actions. The entries list various hosts with their IP addresses, segments (CNC), and functions (Unknown). Below the table, a detailed view for a selected host is shown, including its IPv4 Address (10.44.2.31), MAC Address (000000040077), Operating System (Linux), and Vendor and Model (VMware). The detailed view also shows that the host matched the "Malicious Hosts" policy on June 18 03:35:02 PM and that the main rule condition is "Malicious Event" with the action "Port scan".

- To customize the information displayed about hosts and users connected to endpoints, right-click a column heading, select **Add/Remove Columns**, and select the information of interest to you. You can also reorder the columns.

## Generate Reports

After the policy runs, you can generate reports with real-time and trend information about hosts that are under threat of attacks. You can generate and view the reports immediately, or schedule report generation.

 *The Reports Portal provides tools to customize reports and schedule automatic report generation. For more information about this portal, see the CounterACT Administration Guide.*

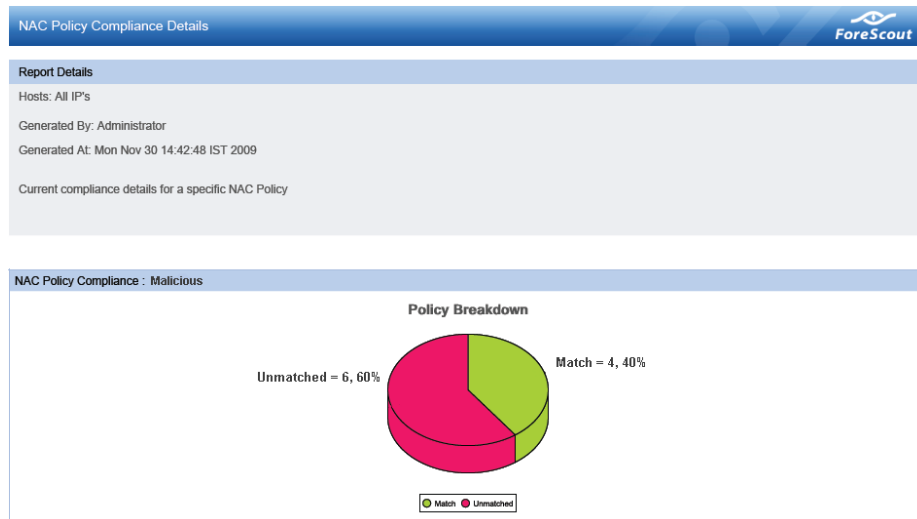
### To generate a report:

- Select **Web Reports** from the Console **Reports** menu. The Reports portal opens.
- Select **Add**. The Add Report Template dialog box opens.
- Select a report template, and select **Next**. A report configuration page opens.
- Define the report specifications in each field.
- Schedule report generation (optional).
- Select **Save** (optional) to save the report settings and assign them a name. The report name appears in the **Reports** list for future use.
- Select **Run** to generate and display the report.





In the following example, the Policy Compliance Details report was selected. This report gives you a pie chart breakdown of network assets. It also provides details about each asset, depending on the information fields you selected to view.



## 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](http://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.

The screenshot shows the 'Options' menu on the left with 'Licenses' selected. The main area displays the 'Licenses' section with a search bar and a table of licenses. The table has columns for Name, Status, and Type. The first row, 'ForeScout CounterACT See', is highlighted in blue and has a red underline. Its status is 'Valid, Capacity exceeded' and its type is 'Perpetual'. Other licenses include 'ForeScout CounterACT Control', 'ForeScout CounterACT Resiliency', and 'ForeScout Extended Module for Check Point Next...'. The status for the last three is 'Valid' and their type is 'Perpetual'.

Name ^	Status	Type
<u>ForeScout CounterACT See</u>	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

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



## Legal Notice

© 2018 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.

2018-04-15 10:56