ForeScout CounterACT®

Prevent Network Attacks

How-to Guide

Version 8.0

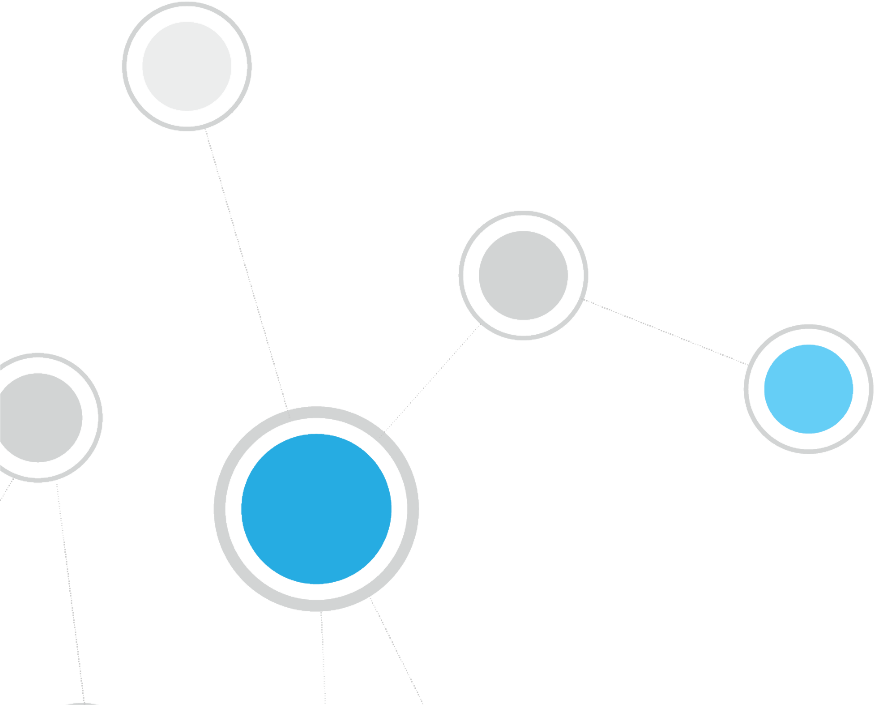


Table of Contents

About Preventing Network Attacks

ForeScout CounterACT® 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.

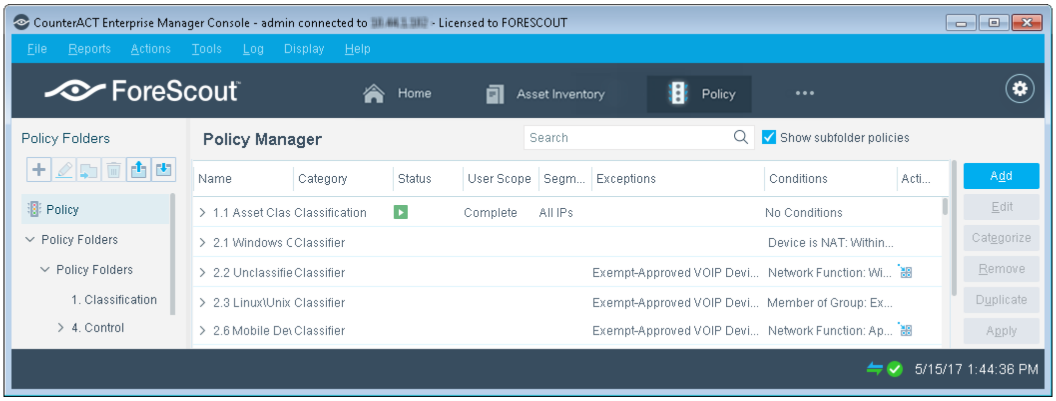
Create and Apply a Threat Protection Policy

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.

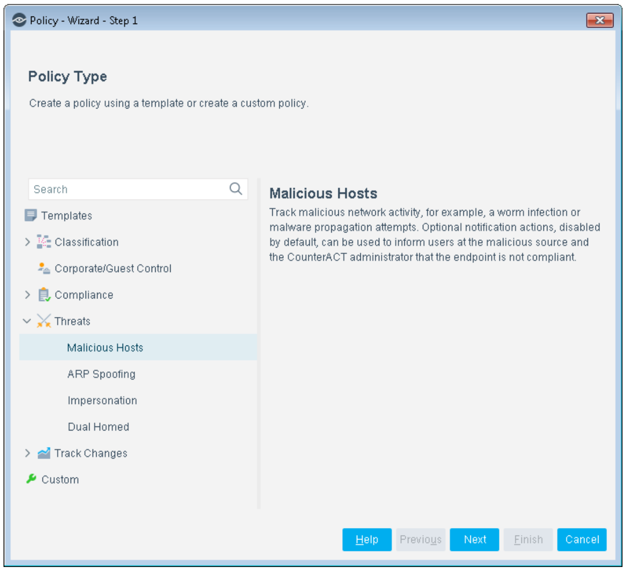
1 Select the Malicious Hosts Template

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



Name	Category	Status	User Scope	Segm...	Exceptions	Conditions	Acti...
1.1 Asset Clas Classification		▶	Complete	All IPs		No Conditions	
2.1 Windows C Classifier						Device is NAT: Within...	
2.2 Unclassifie Classifier					Exempt-Approved VOIP Devi...	Network Function: Wi...	
2.3 Linux\Unix Classifier					Exempt-Approved VOIP Devi...	Member of Group: Ex...	
2.6 Mobile De Classifier					Exempt-Approved VOIP Devi...	Network Function: Ap...	

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



Policy Type

Create a policy using a template or create a custom policy.

Malicious Hosts

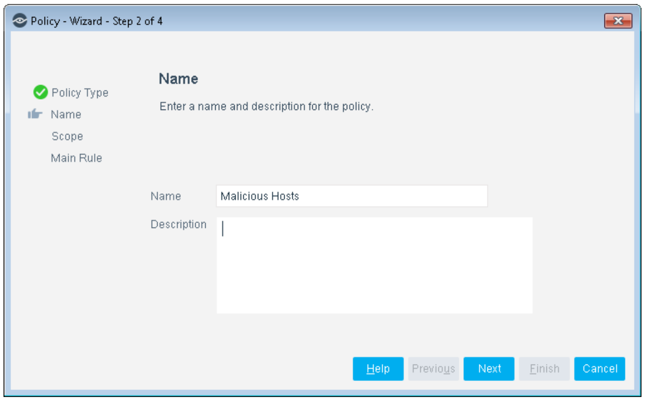
Track malicious network activity, for example, a worm infection or malware propagation attempts. Optional notification actions, disabled by default, can be used to inform users at the malicious source and the CounterACT administrator that the endpoint is not compliant.

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.



Policy - Wizard - Step 2 of 4

Name

Enter a name and description for the policy.

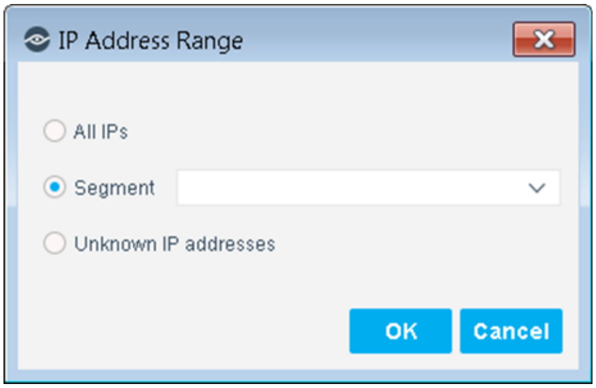
Name: Malicious Hosts

Description:

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.



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

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.

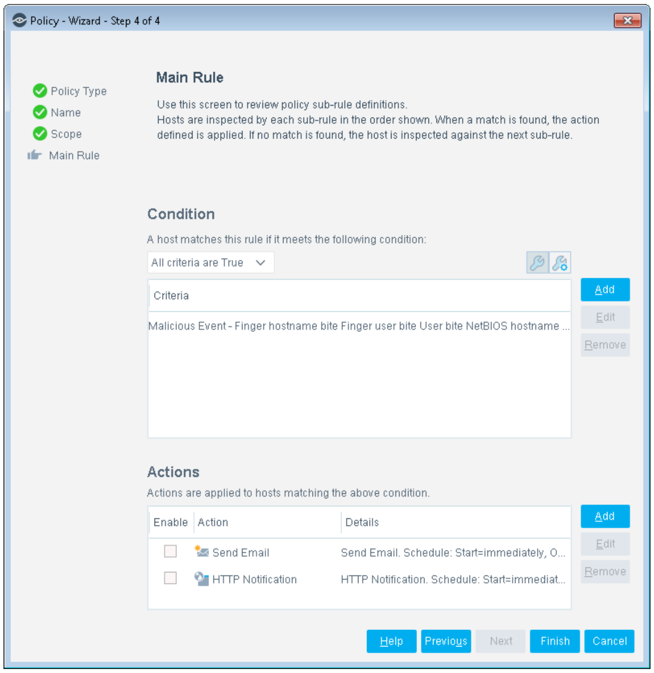
  Not applicable for this policy template.

🗎 *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.



Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Malicious Event - Finger hostname bite Finger user bite User bite NetBIOS hostname ...

Actions

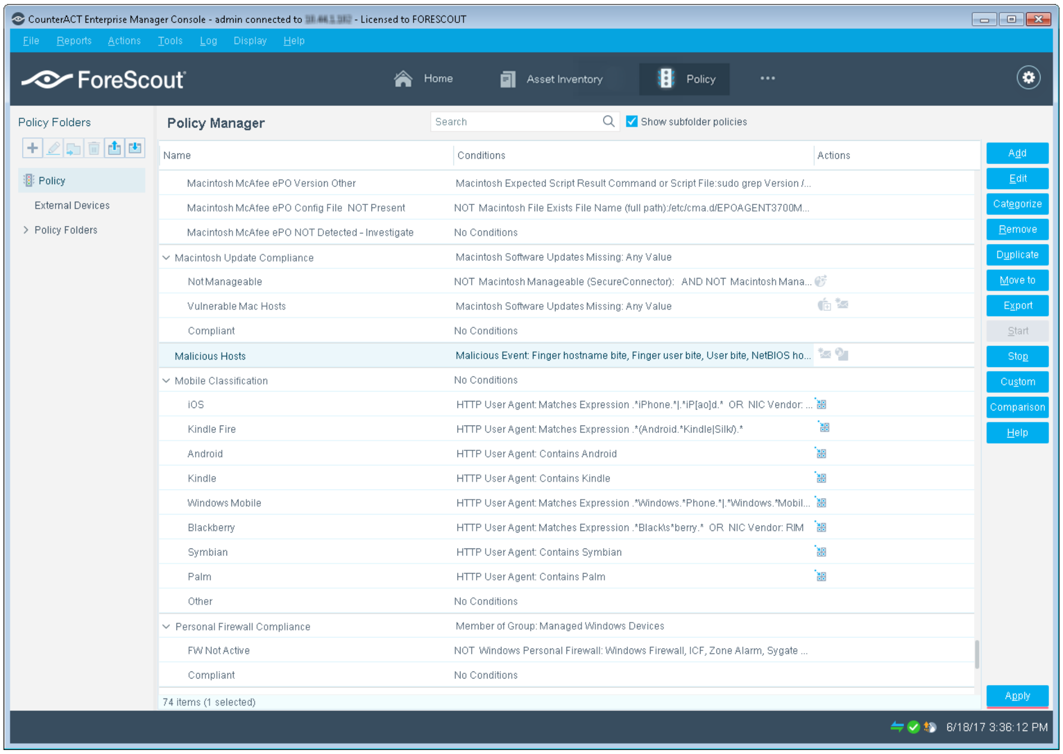
Actions are applied to hosts matching the above condition.

Enable	Action	Details
□	Send Email	Send Email. Schedule: Start=immediately, O...
□	HTTP Notification	HTTP Notification. Schedule: Start=immediat...

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.



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to FORESCOUT

Policy Manager

☑ Show subfolder policies

Name	Conditions	Actions
Macintosh McAfee ePO Version Other	Macintosh Expected Script Result Command or Script File:sudo grep Version /...	
Macintosh McAfee ePO Config File NOT Present	NOT Macintosh File Exists File Name (full path):/etc/cma.d/EPOAGENT3700M...	
Macintosh McAfee ePO NOT Detected - Investigate	No Conditions	
Macintosh Update Compliance	Macintosh Software Updates Missing: Any Value	
Not Manageable	NOT Macintosh Manageable (SecureConnector): AND NOT Macintosh Mana...	
Vulnerable Mac Hosts	Macintosh Software Updates Missing: Any Value	
Compliant	No Conditions	
Malicious Hosts	Malicious Event: Finger hostname bite, Finger user bite, User bite, NetBIOS ho...	
Mobile Classification	No Conditions	
iOS	HTTP User Agent: Matches Expression .*iPhone.*|.*iP[ao]d.* OR NIC Vendor: ...	
Kindle Fire	HTTP User Agent: Matches Expression .*(Android.*Kindle|Silk/).*	
Android	HTTP User Agent: Contains Android	
Kindle	HTTP User Agent: Contains Kindle	
Windows Mobile	HTTP User Agent: Matches Expression .*Windows.*Phone.*|.*Windows.*Mobil...	
Blackberry	HTTP User Agent: Matches Expression .*Black\s*berry.* OR NIC Vendor: RIM	
Symbian	HTTP User Agent: Contains Symbian	
Palm	HTTP User Agent: Contains Palm	
Other	No Conditions	
Personal Firewall Compliance	Member of Group: Managed Windows Devices	
FW Not Active	NOT Windows Personal Firewall: Windows Firewall, ICF, Zone Alarm, Sygate ...	
Compliant	No Conditions	

74 items (1 selected)

6/18/17 3:36:12 PM

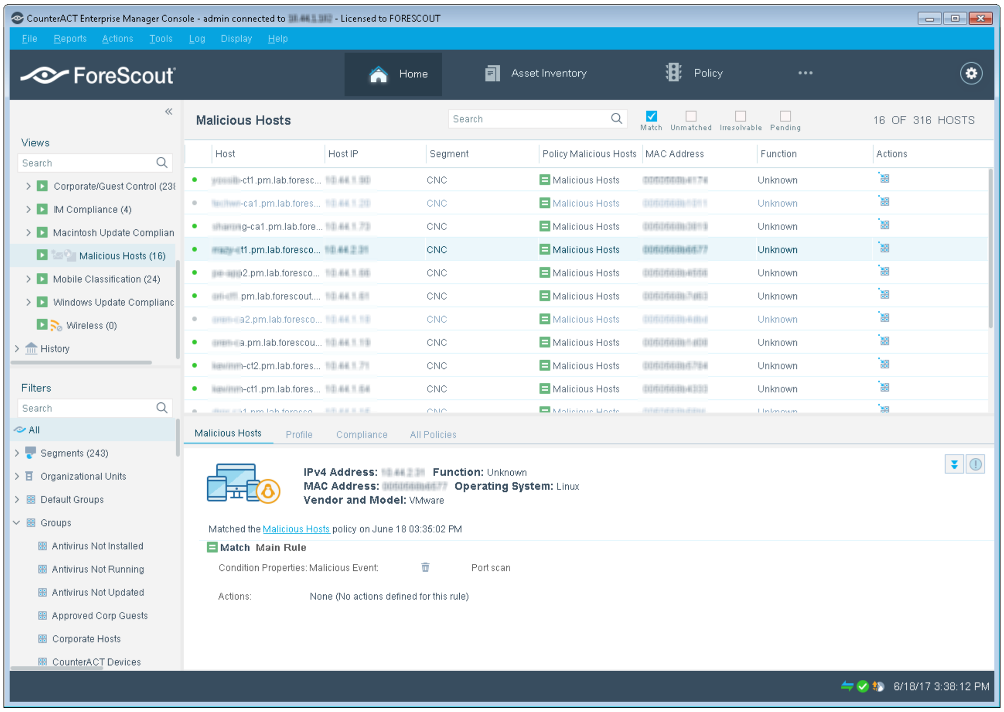
3. Select **Apply**. The policy is activated.

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.



Malicious Hosts

16 OF 316 HOSTS

Host	Host IP	Segment	Policy Malicious Hosts	MAC Address	Function	Actions
[redacted]-ct1.pm.lab.foresc...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]-ca1.pm.lab.fores...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]g-ca1.pm.lab.fore...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]t1.pm.lab.foresco...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]2.pm.lab.foresco...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted] pm.lab.forescout....	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]a2.pm.lab.foresco...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]a.pm.lab.forescou...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]-ct2.pm.lab.fores...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	
[redacted]-ct1.pm.lab.fores...	[redacted]	CNC	Malicious Hosts	[redacted]	Unknown	

IPv4 Address: [redacted] **Function:** Unknown
MAC Address: [redacted] **Operating System:** Linux
Vendor and Model: VMware

Matched the Malicious Hosts policy on June 18 03:35:02 PM

Match Main Rule

Condition Properties: Malicious Event: Port scan

Actions: None (No actions defined for this rule)

4. 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

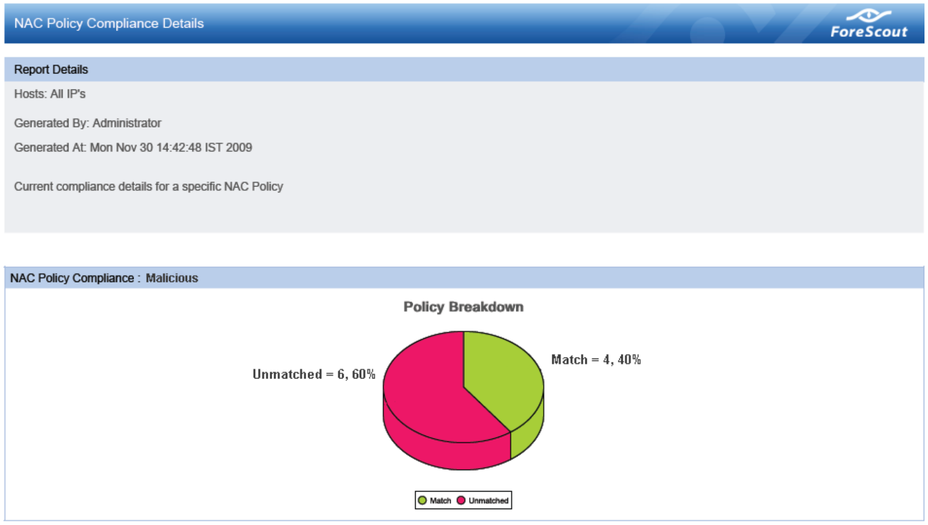
After the policy runs, you can generate reports with real-time and trend information about hosts that are under threat of attacks. You can generate and view the reports immediately, or schedule report generation.

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:

1. Select **Web Reports** from the Console **Reports** menu. The Reports portal opens.
2. Select **Add**. The Add Report Template dialog box opens.
3. Select a report template, and select **Next**. A report configuration page opens.
4. Define the report specifications in each field.
5. Schedule report generation (optional).
6. Select **Save** (optional) to save the report settings and assign them a name. The report name appears in the **Reports** list for future use.
7. 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.



NAC Policy Compliance Details

ForeScout

Report Details

Hosts: All IP's

Generated By: Administrator

Generated At: Mon Nov 30 14:42:48 IST 2009

Current compliance details for a specific NAC Policy

NAC Policy Compliance : Malicious

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**.

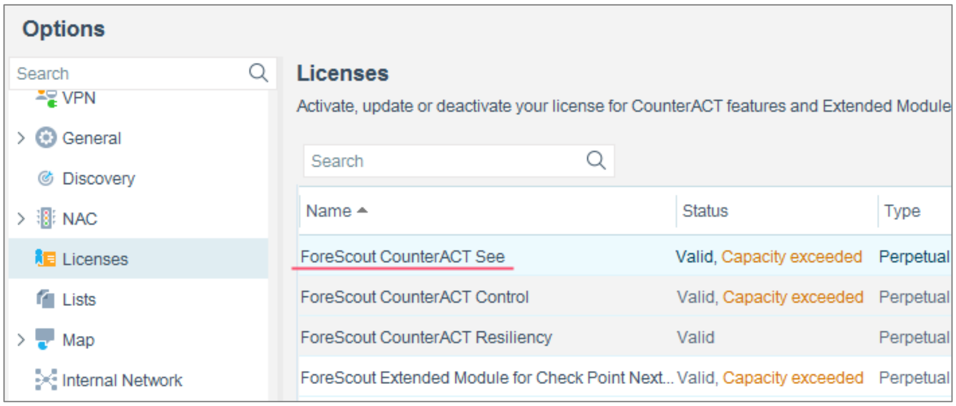
Documentation Portal

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.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	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

2018-04-15 10:56