



ForeScout CounterACT[®]

Track Changes to Network Endpoints

How-to Guide

Version 8.0

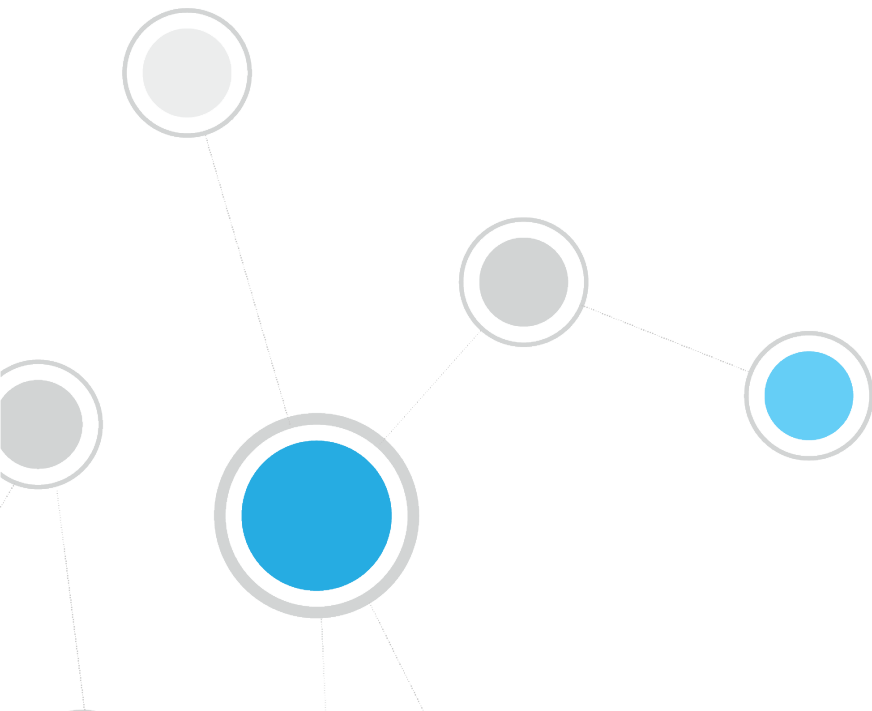




Table of Contents

About Managing Changes to Network Endpoints	3
Prerequisites	3
Create and Apply a Change Policy	4
Evaluate the Changes	8
Generate Reports	9
Additional CounterACT Documentation	10
Documentation Downloads	10
Documentation Portal	11
CounterACT Help Tools.....	11




About Managing Changes to Network Endpoints

ForeScout CounterACT® tools let you identify an extensive range of host changes in your network, including changes to:


- Applications installed
- Hostnames
- Operating systems
- Shared folders
- Switches
- Users
- Windows services
- New TCP/IP ports

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

- Use a wizard-based CounterACT template to create a policy that detects and classifies changes to network endpoints.

 *As an example of changes tracked, this guide discusses NetBIOS hostname changes.*

- Use CounterACT tools to review an extensive range of information about detected hosts.
- Generate real-time and trend reports tracking changes.

 *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.



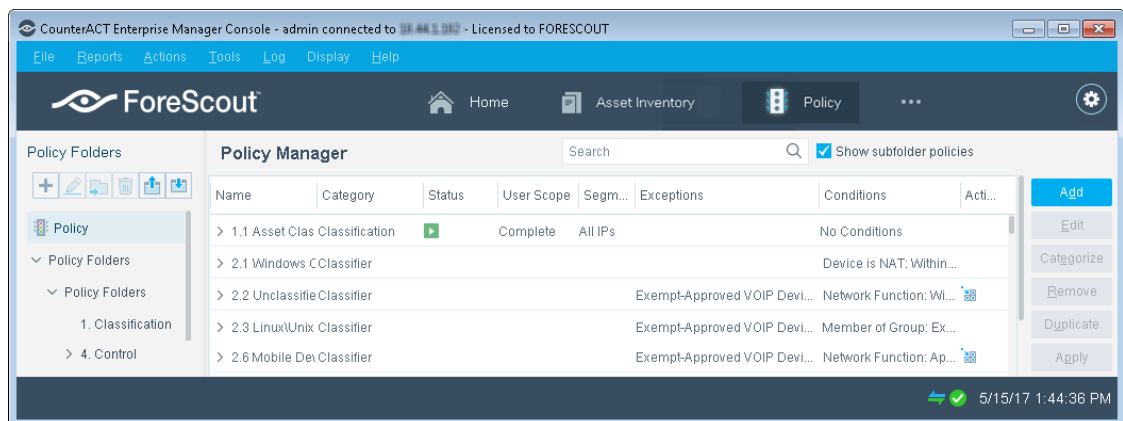
Create and Apply a Change Policy

Follow the steps below to detect hostname changes using a policy template.

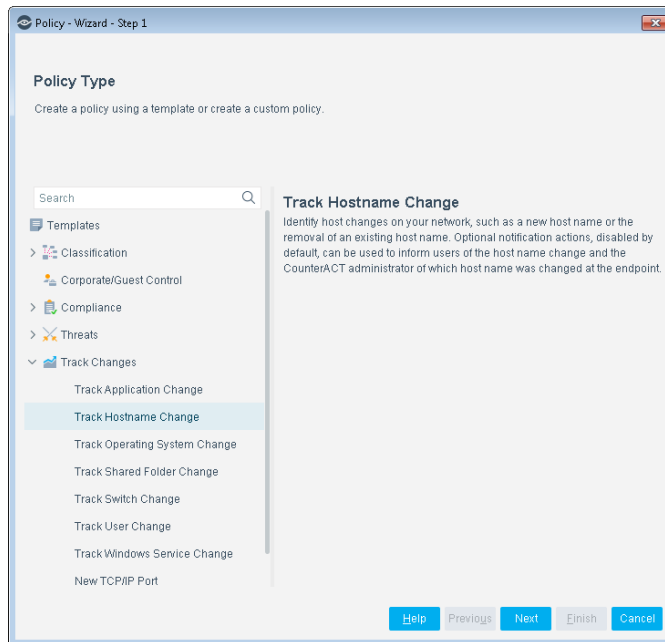
- 📄 *This guide discusses how to track and control hostname changes specifically, but it also applies to all other changes listed in [About Managing Changes to Network Endpoints](#).*

1 Select a Track Change Template

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



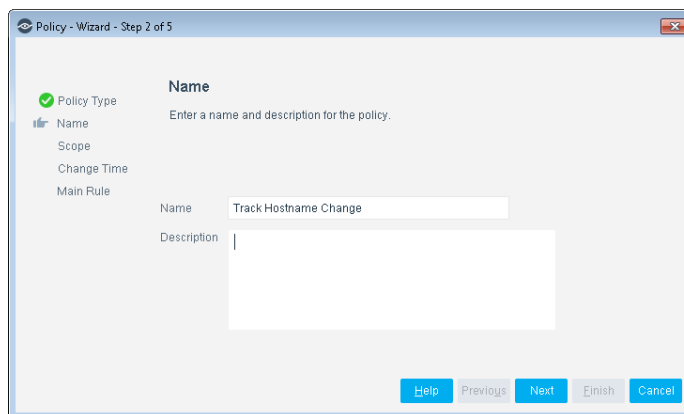
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Track Changes** folder and select **Track Hostname Change** (or the template you require).



5. Select **Next**. The 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 open.

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**.*

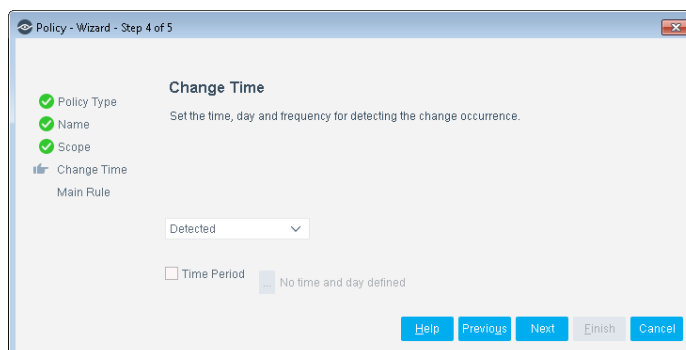
2. Select **OK**. The added range appears in the Scope list.
3. Select **Next**. The Change Time pane opens.



Set Time Criteria for Detected Changes

In the Change Time pane, set the time criteria for detected changes.

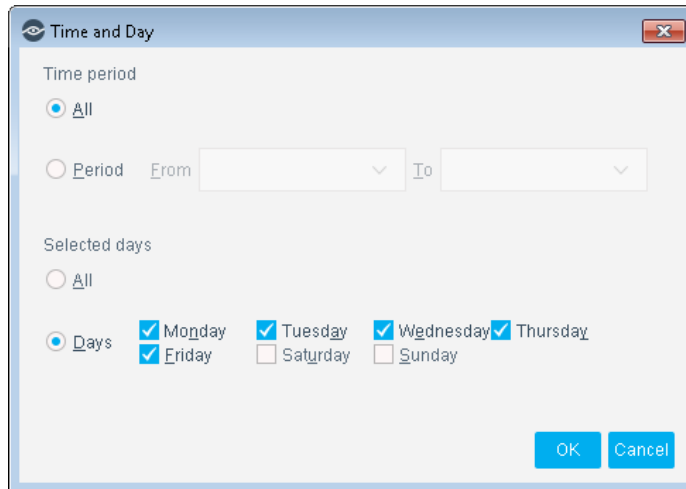
1. In the **Detected** drop-down list, set the beginning or ending date for the changes to be detected (optional).



2. To limit the detection to changes made during specific days or hours, select **Time Period**. The Time and Day dialog box opens.



In the following example, hostname changes will be detected if they occurred from Monday through Friday, at any time of day, within the previous two weeks.

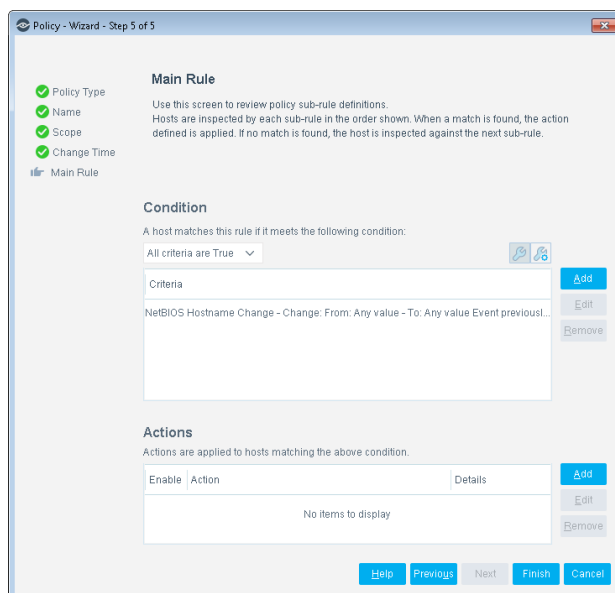


3. Select **OK**.
4. Select **Next**. The Main Rule pane opens.



5 Finish Policy Creation

The policy sub rules are displayed in the Main Rule pane. Rules instruct CounterACT what to detect on hosts (Conditions) and how to handle hosts (Actions).

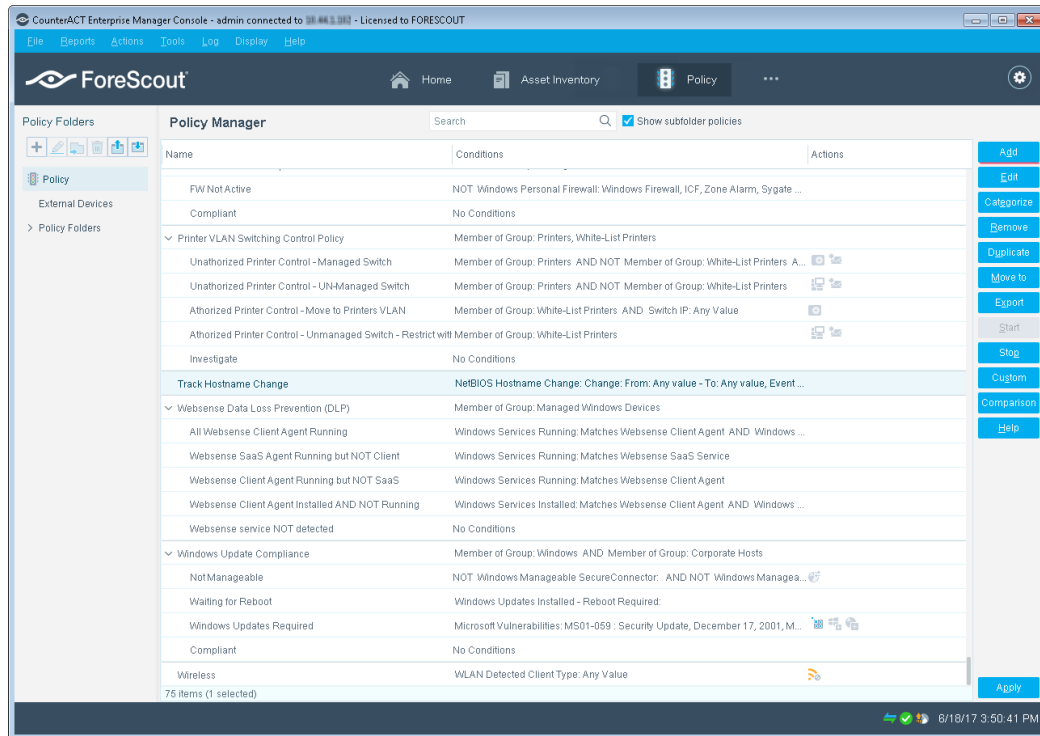


1. Select **Finish**. The policy automatically appears highlighted in the Policy Manager, where it can be activated.



6 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.

CounterACT detects hostname changes at the addresses you specified in the Scope pane, within the time periods you specified.

Evaluate the Changes

After activating the policy, you can view details about endpoints at which the changes were detected.

To evaluate the detected changes:

4. On the Console toolbar, select the Home tab.
5. In the Views pane, expand the **Policy** folder and select the policy containing your change policy.



The screenshot displays the CounterACT Enterprise Manager Console interface. The main window shows a table titled "Track Hostname Change" with 315 hosts. The table columns include Host, HostIP, Segment, Policy Track Hostname, MAC Address, Function, and Actions. A detailed view for a specific host is shown below the table, displaying its IP4 Address (10.44.1.247), Function (Networking), MAC Address (08000604704e), Operating System (Unknown), and Vendor and Model (Cisco). A notification indicates that the host did not match the "Track Hostname Change" policy on June 18, 2017, at 03:49:26 PM, with the reason being "Change was not detected irrevocable".

Host	HostIP	Segment	Policy Track Hostname	MAC Address	Function	Actions
pm-@junk.pm.lab.foresc...	10.44.1.22	CNC	Track Hostname C...		Unknown	
pm-@m1-63410.pm.lab.f...	10.44.1.54	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@m1.pm.lab.forescou...	10.44.1.41	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@3.pm.lab.forescou...	10.44.1.59	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@2.pm.lab.forescou...	10.44.1.247	CNC	Track Hostname C...	08000604704e	Networking	
pm-@edge-natl.pm.lab.f...	10.44.1.272	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@m2.pm.lab.forescou...	10.44.1.55	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@m1.pm.lab.forescou...	10.44.1.23	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@ip2.pm.lab.forescou...	10.44.1.56	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@m1.pm.lab.forescou...	10.44.1.50	CNC	Track Hostname C...	08000604704e	Unknown	
pm-@m1.pm.lab.forescou...	10.44.1.29	CNC	Track Hostname C...	08000604704e	Unknown	

6. Change information is displayed in the Detections pane.
7. To customize the information displayed about detected changes, 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 tracked changes. 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.

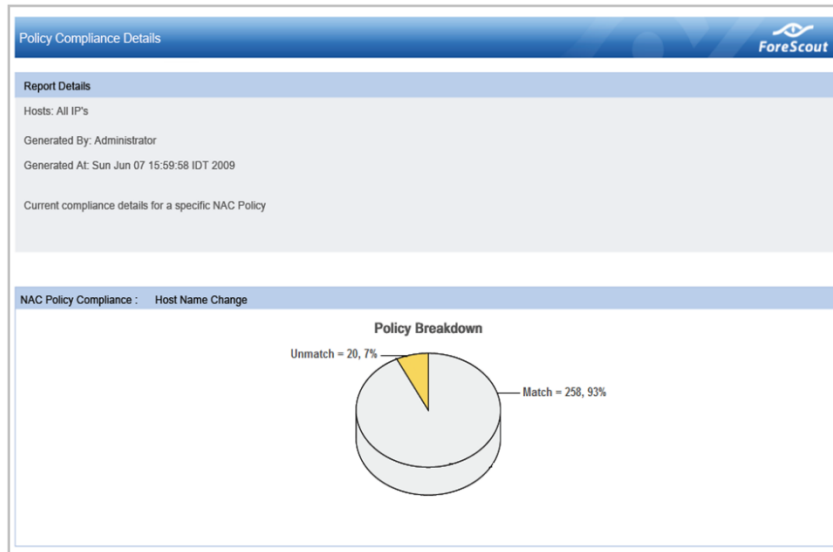
To generate a report:

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 hostname changes, and provides details 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.
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.

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 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 11:07