ForeScout

Track Changes to Network Endpoints

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Managing Changes to Network Endpoints

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 Console User Manual or the Console Online Help.

Prerequisites

- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.

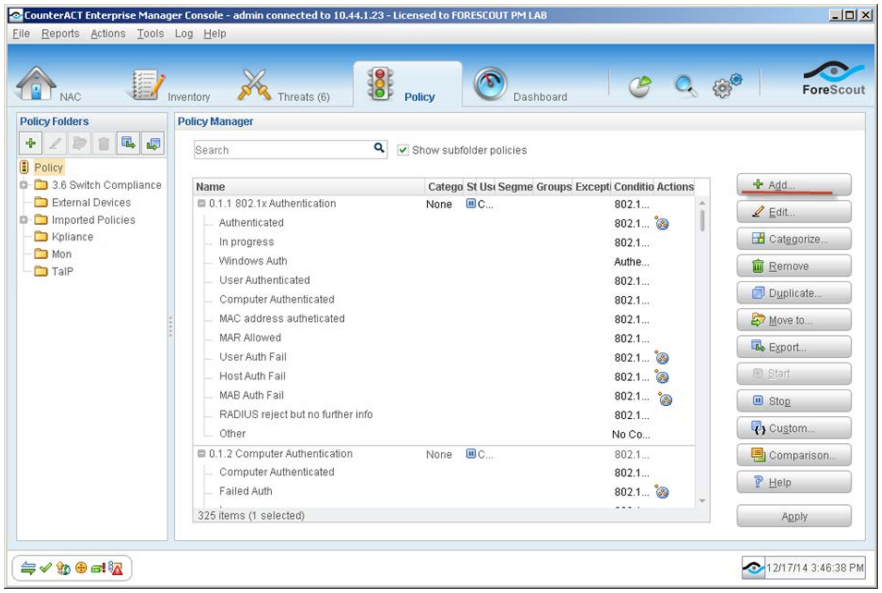
Create and Apply a Change Policy

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

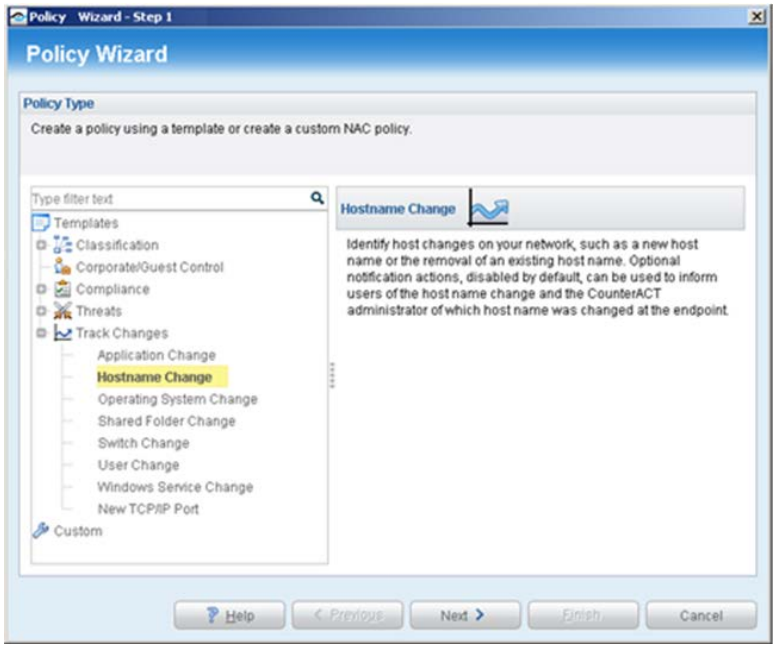
This guide discusses how to track and control hostname changes specifically, but it also applies to all other changes listed in About Managing Changes to Network Endpoints.

Select a Track Change Template

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



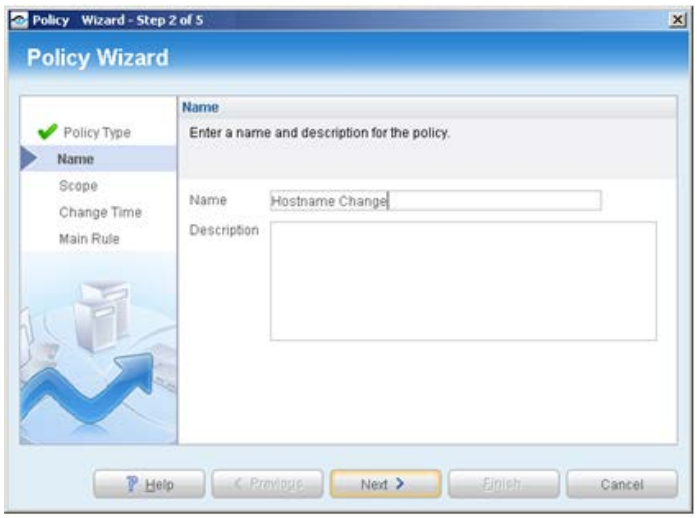
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Track Changes** folder and select **Hostname Change** (or the template you require).



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

2 Name the Policy

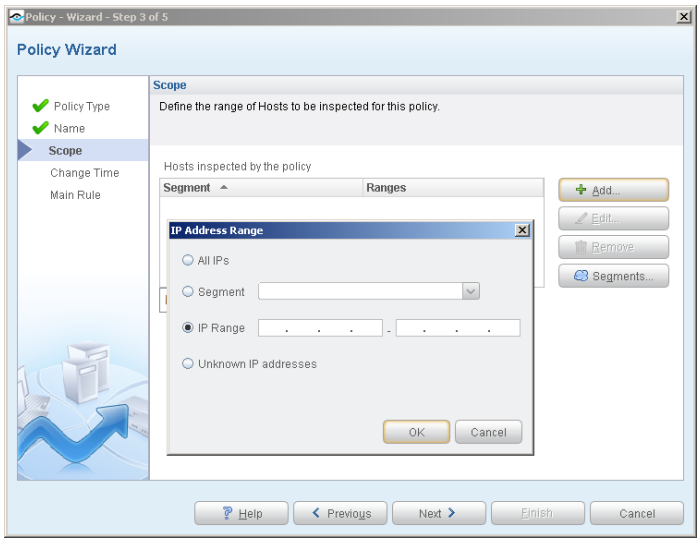
1. In the Name pane, a default policy name appears in the **Name** field.



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 the IP addresses you want to inspect.



The following options are available:

- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments** Segments... from the Scope pane.
- **IP Range** lets you define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses** applies the policy to hosts whose IP addresses are not known. Not applicable for this policy template.

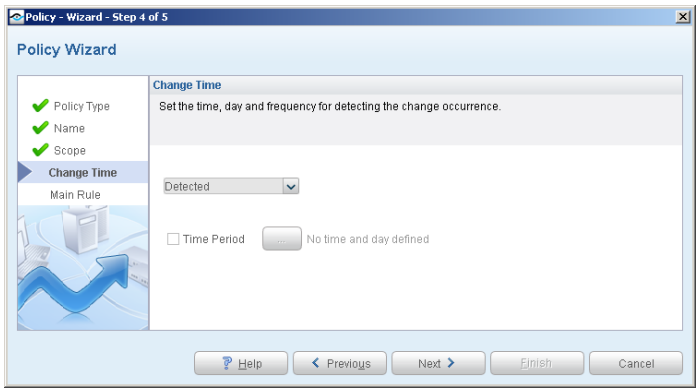
Viewing or modifying the Internal Network is performed separately. Select Tools>Options>Internal Network.

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

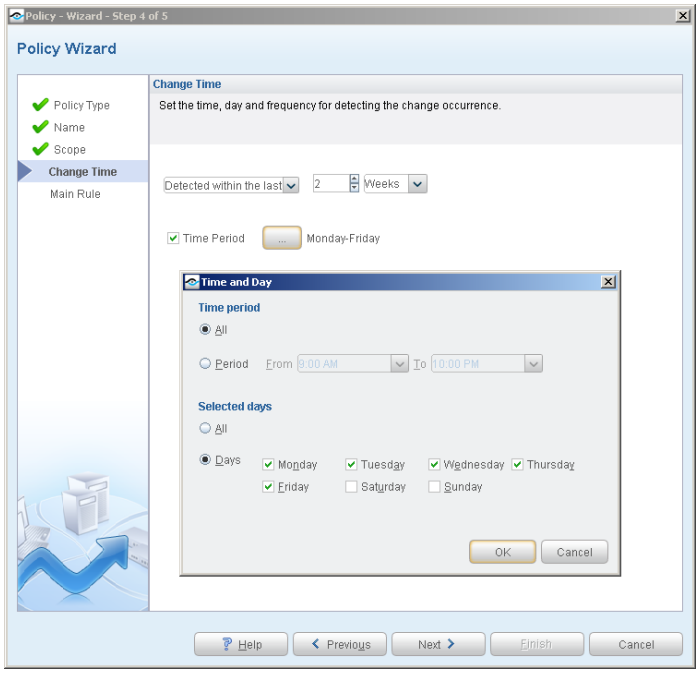
In the Change Time pane, set the time criteria for detected changes.

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.

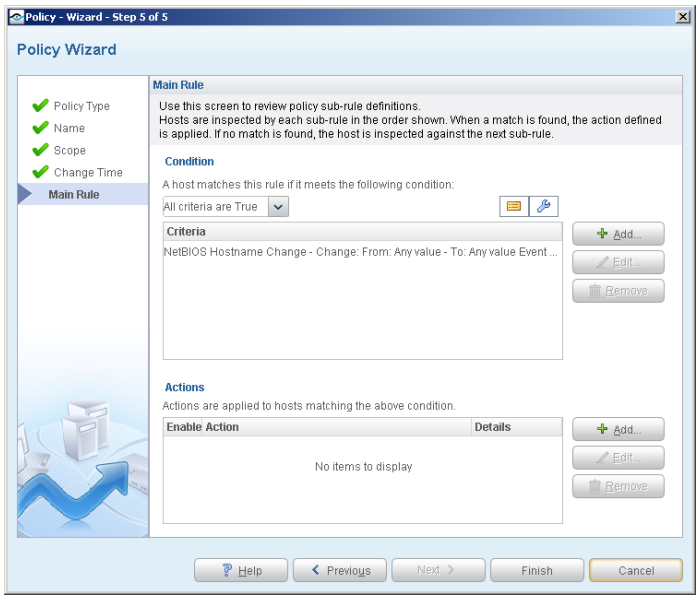
   In the following example, hostname changes will be detected if they occurred from Monday through Friday, at any time of day, within the previous two weeks.



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

5 Finish Policy Creation

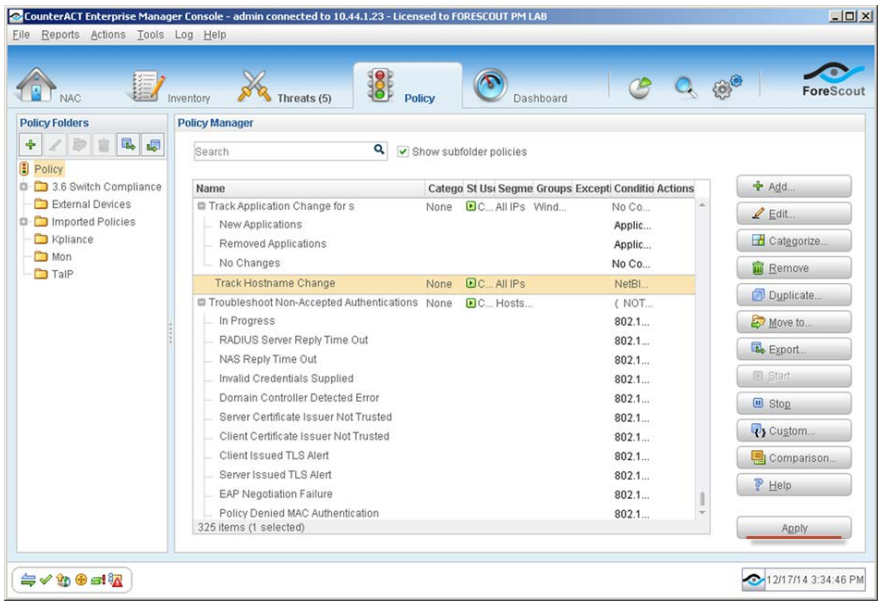
The policy sub rules are displayed in the Main Rule pane. Rules instruct CounterACT what to detect on hosts (Conditions) and how to handle hosts (Actions).



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.

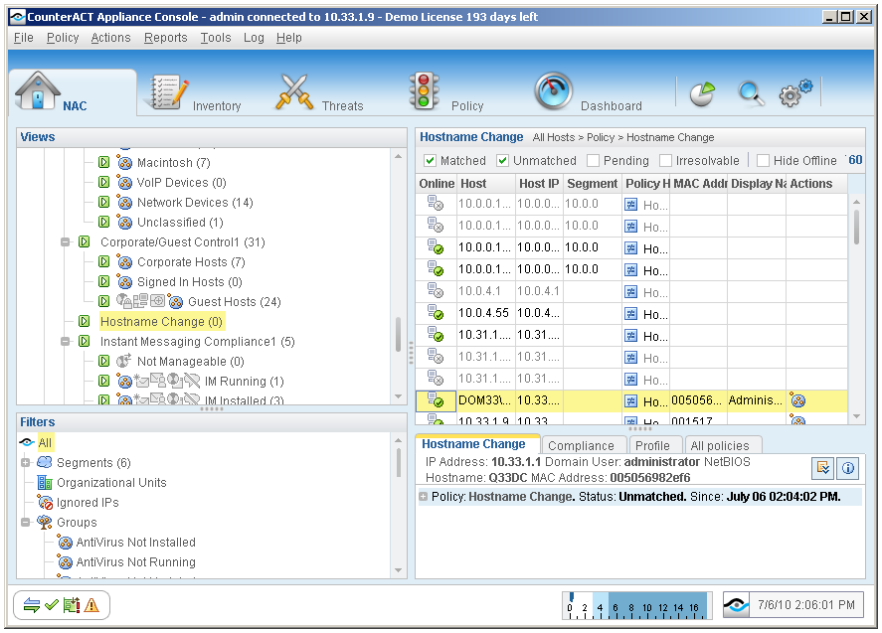
   CounterACT detects hostname changes at the addresses you specified in the Scope pane, within the time periods you specified.

Evaluate the Changes

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

To evaluate the detected changes:

1. On the Console toolbar, select the NAC tab.
2. In the Views pane, expand the **Policy** folder and select the policy containing your change policy.



3. Change information is displayed in the Detections pane.
4. 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

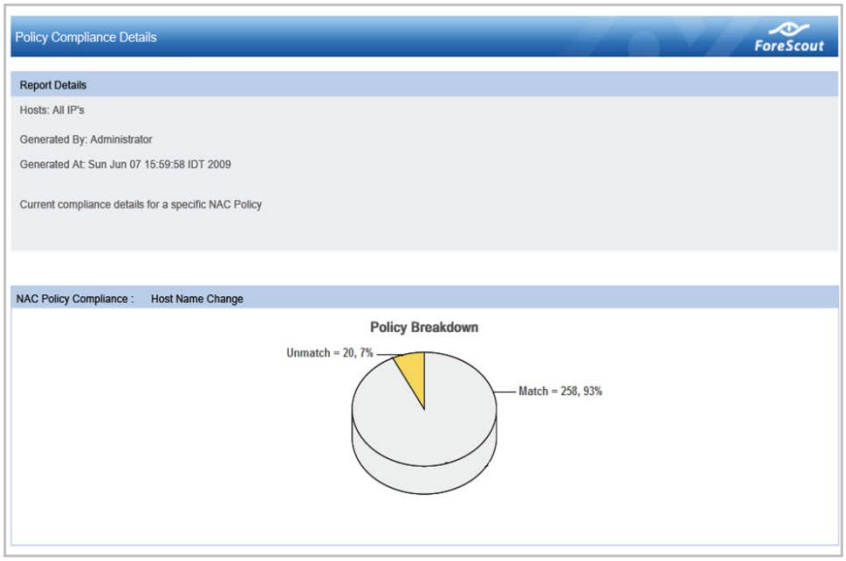
After the policy runs, you can generate reports with real-time and trend information about tracked changes. You can generate and view the reports immediately, or generate schedules to ensure that changes are automatically and consistently reported.

The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User 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.



Legal Notice