FORESCOUT

Forescout

Track Changes to Network Endpoints

How-to Guide

Forescout version 8.1

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

Legal Notice

2019-03-20 14:25

Table of Contents

About Managing Changes to Network Endpoints

Forescout® 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 Forescout 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 Forescout 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 Forescout Administration Guide.

Prerequisites

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

Create and Apply a Change Policy

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

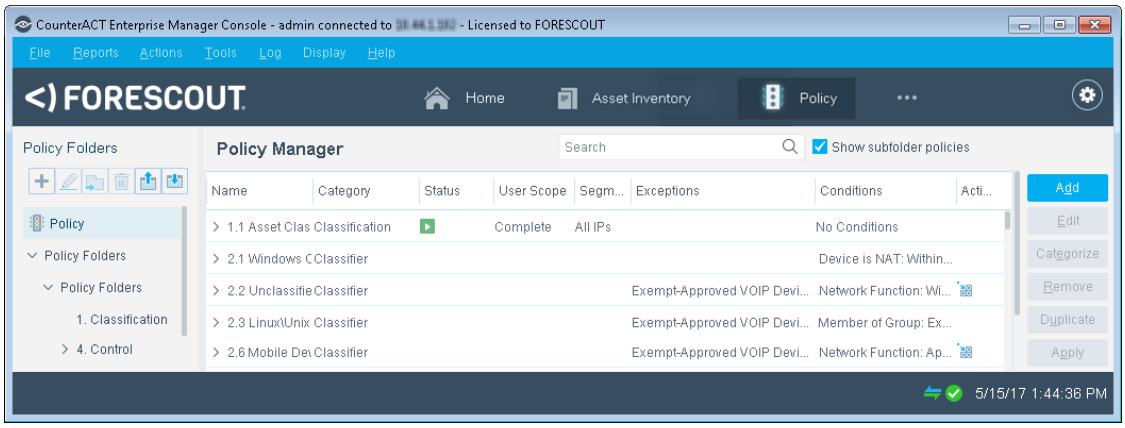
- Select a Track Change Template
- Name the Policy
- Choose Host to Inspect
- Set Time Criteria for Detected Changes
- Finish Policy Creation
- Activate the Policy

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

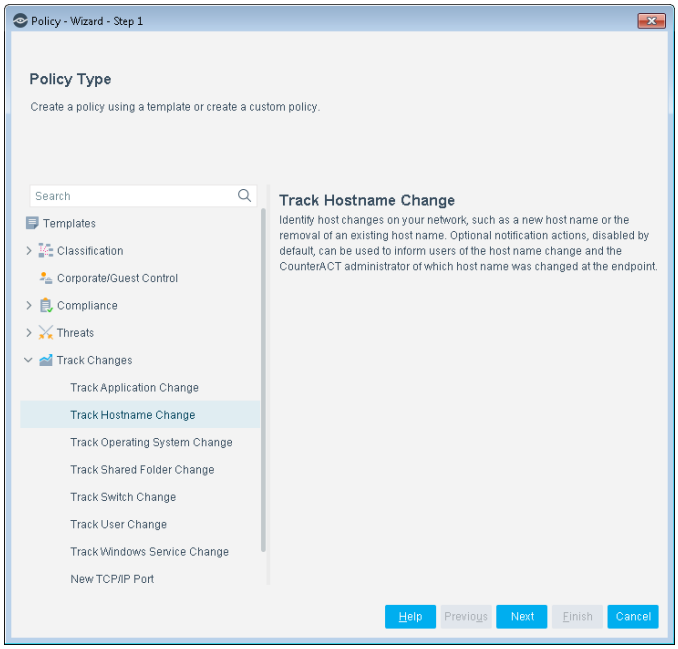
To select a Track Change template:

1. Log into the Forescout 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).

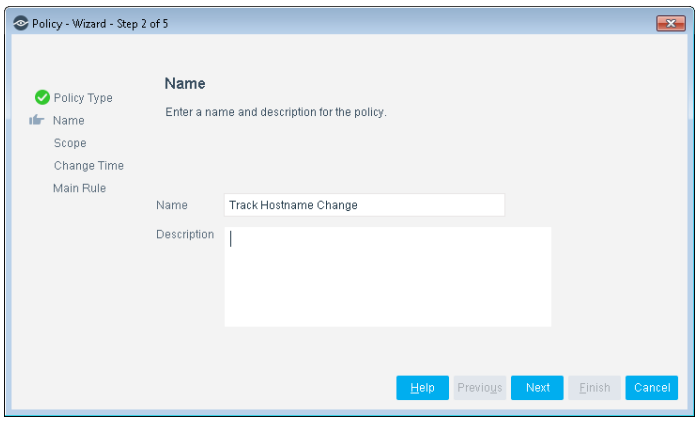


5. Select **Next**. The Name pane opens.

Name the Policy

To name the policy:

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

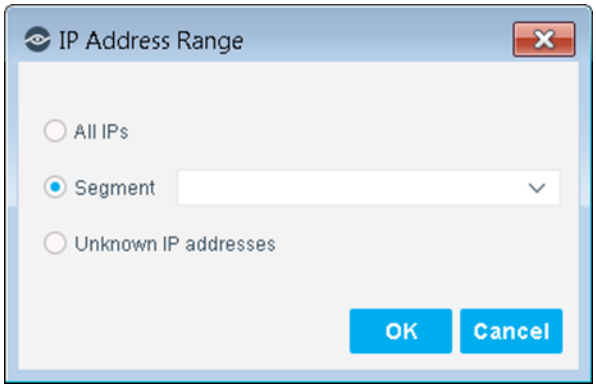


2. Accept the default name or create a new name, and add a description.
3. Select **Next**. The Scope pane and the IP Address Range dialog box open.

Choose Host to Inspect

To choose host 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 pane.
- **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.

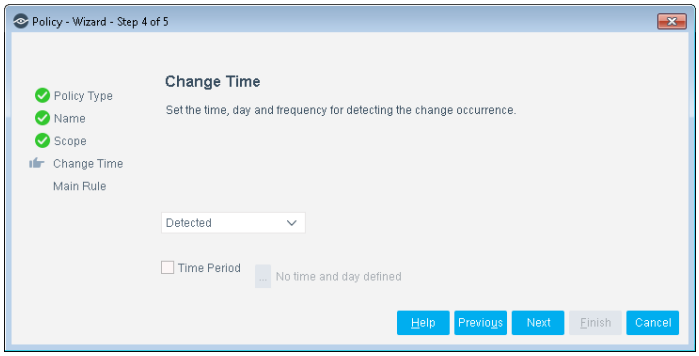
2. Select **OK**. The added range appears in the Scope list.
3. Select **Next**. The Change Time pane opens.

Set Time Criteria for Detected Changes

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

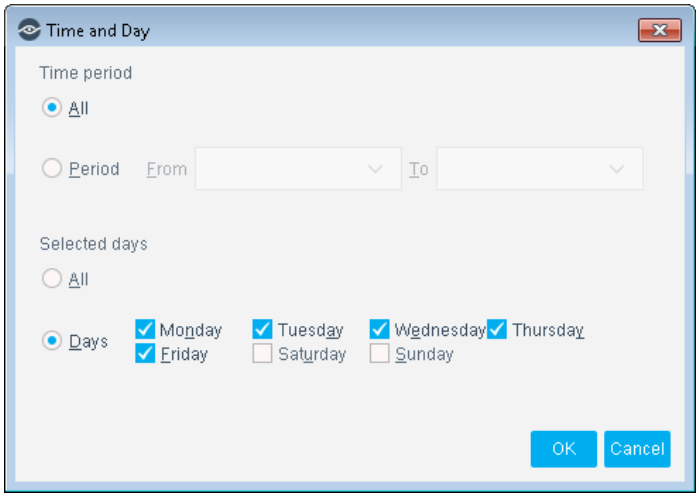
To set the time criteria for detected changes:

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.

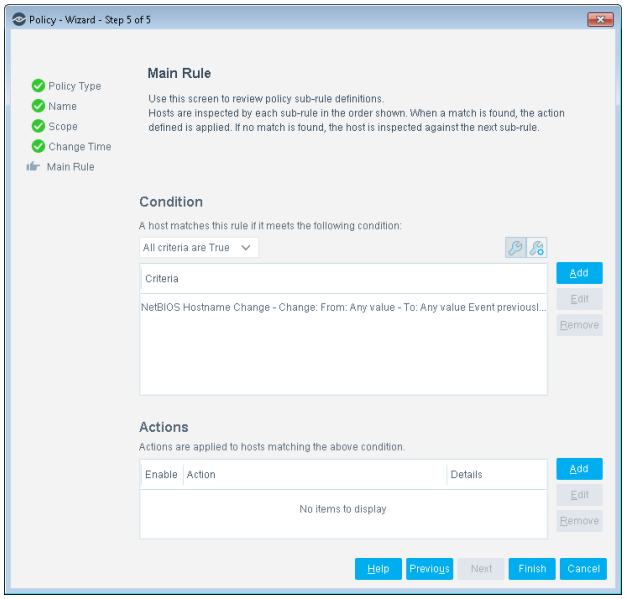
   In the following example, hostname changes will be detected if they occurred from Monday through Friday, at any time of day, within the previous two weeks.



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

Finish Policy Creation

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



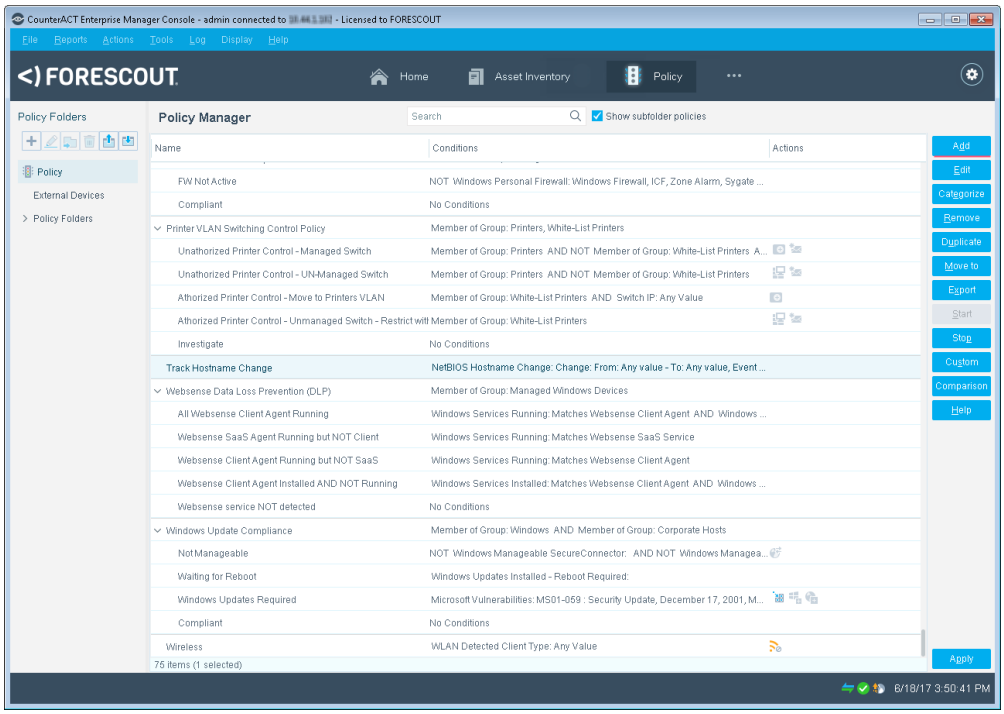
To finish creating the policy:

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

Activate the Policy

To 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.

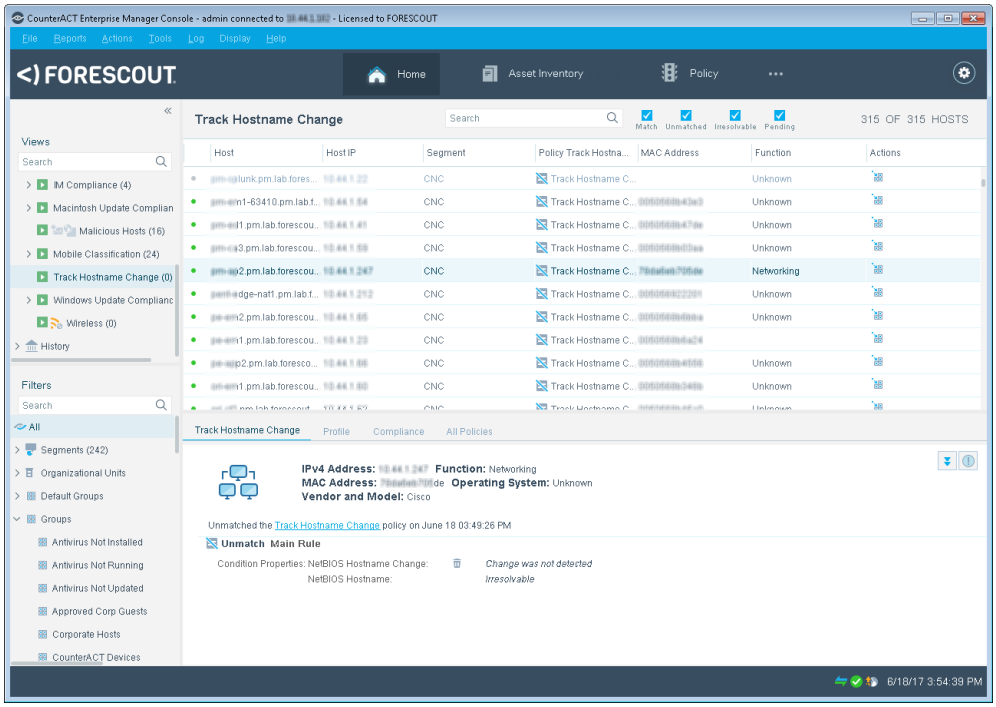
   The Forescout platform detects hostname changes at the addresses you specified in the Scope pane, within the time periods you specified.

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 Home 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

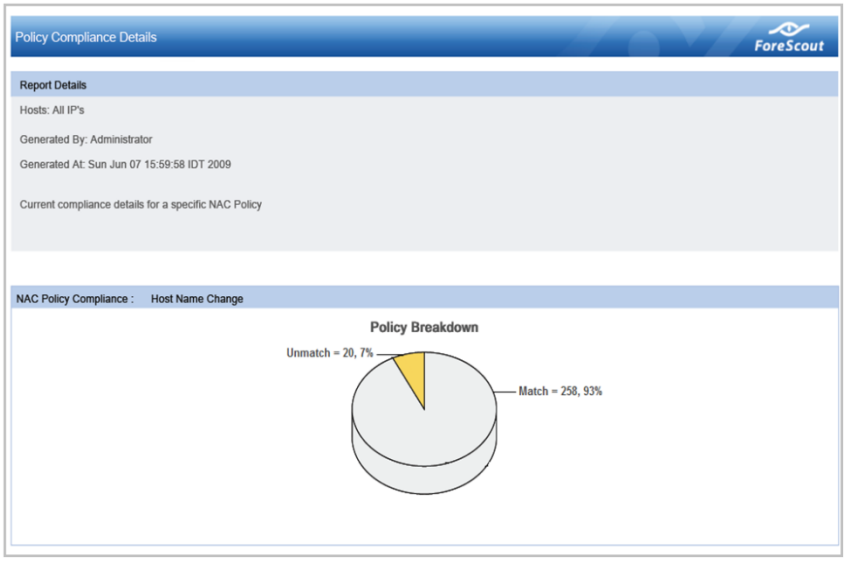
After the policy runs, you can generate reports with real-time and trend information about tracked changes. You can generate and view the reports immediately, or schedule report generation.

The Reports Portal provides tools to customize reports and schedule automatic report generation. For more information about this portal, see the Forescout 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 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, or 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 will 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.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

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

Plugin Help Files

- After the plugin is installed, 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).