FORESCOUT

Forescout

Prevent Network Attacks

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 14:21

Table of Contents

About Preventing Network Attacks

Forescout® 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 Forescout 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 Forescout 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 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 Threat Protection Policy

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

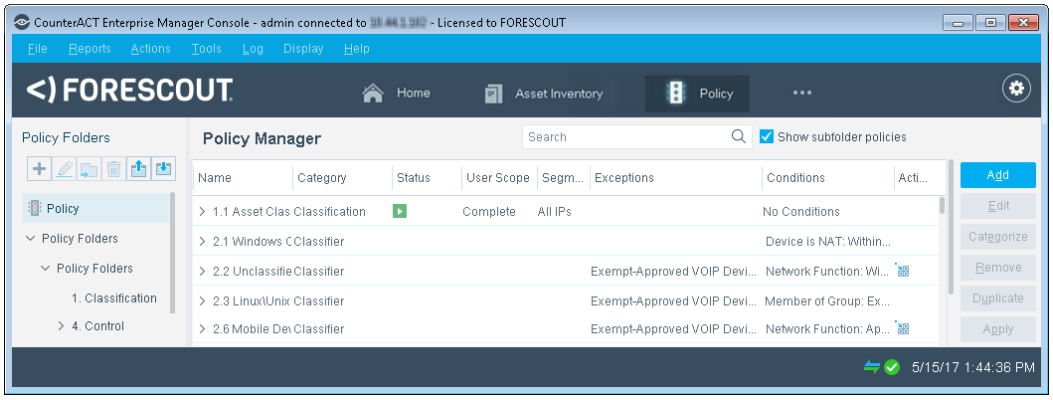
- Select the Malicious Host Template
- Name the Policy
- Choose the Host to Inspect
- Finish Policy Creation
- Activate the Policy

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

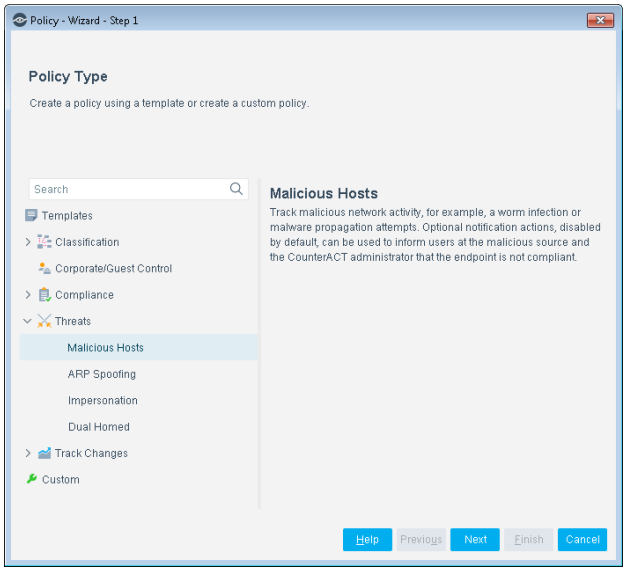
Select the Malicious Host Template

To select the Malicious Host 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 pane select **Add**. The Policy Wizard opens, guiding you through policy creation.

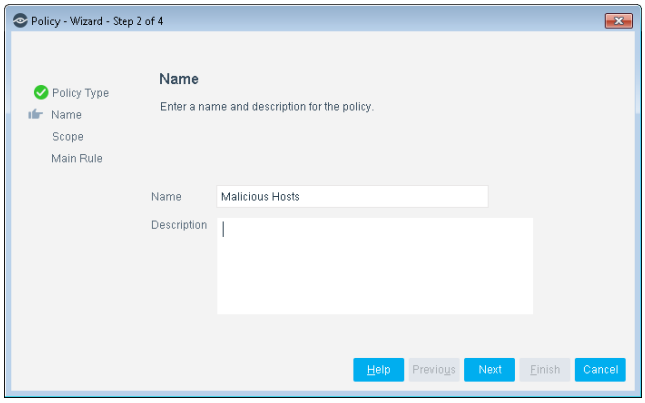


4. Under **Templates**, expand the **Threats** folder and select **Malicious Hosts**.
5. Select **Next**. The Policy Name pane opens.

Name the Policy

To name the policy:

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

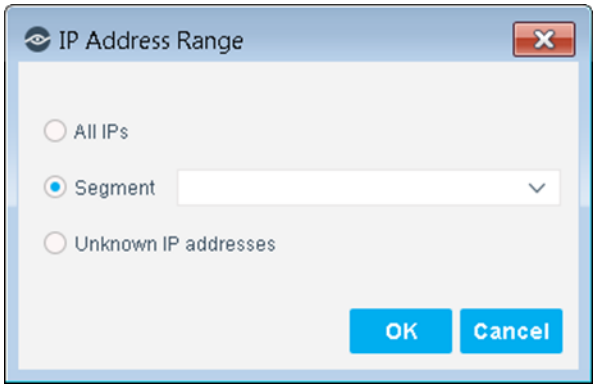


2. Accept the default name or create a new name, and add a description.
3. Select **Next**. The Scope pane and the IP Address Range dialog box opens.

Choose the Host to Inspect

To choose the 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.

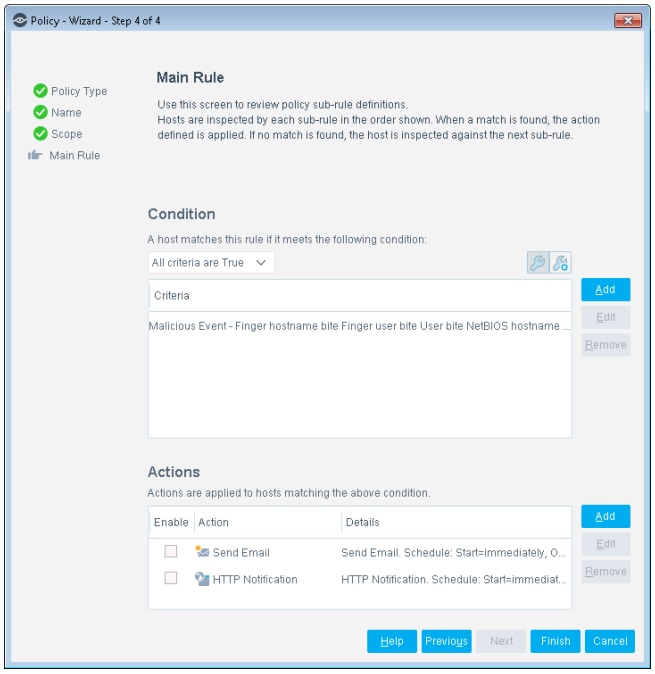
Viewing or modifying the Internal Network is performed separately. Select Tools>Options>Internal Network.

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

Finish Policy Creation

The policy main rules are displayed in the Main Rule pane. Rules instruct the Forescout platform how to detect hosts (Condition) and handle hosts (Actions). Optional notification actions, disabled by default, can be used to notify endpoint users or the Forescout 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.



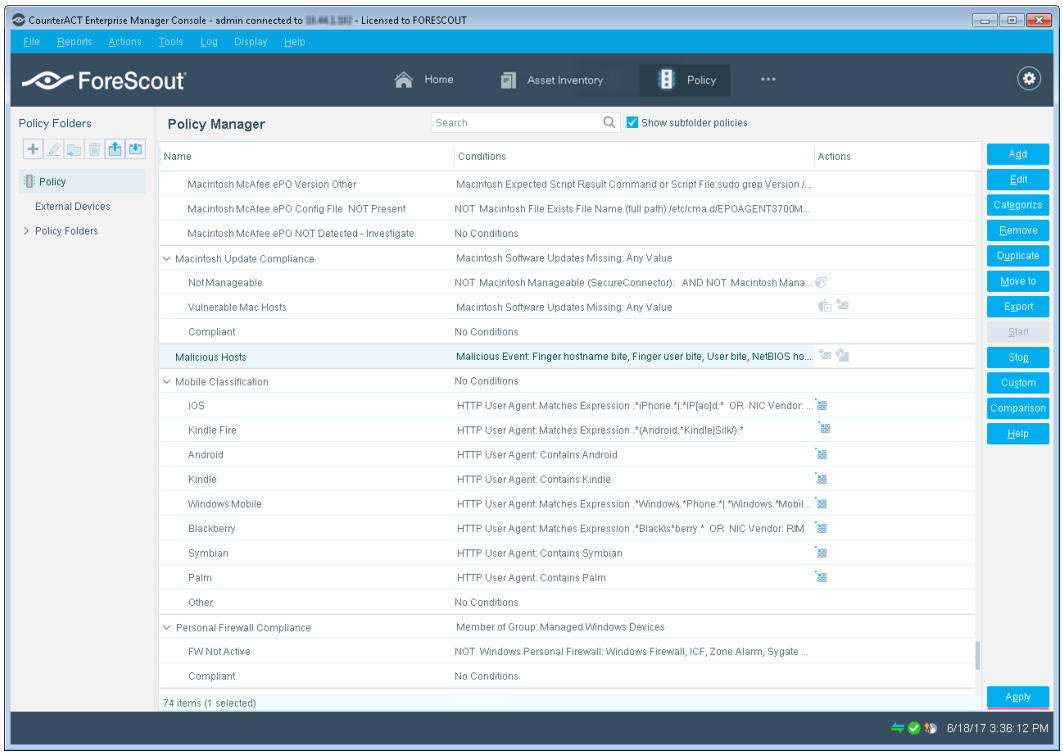
To finish creating the policy:

- 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.

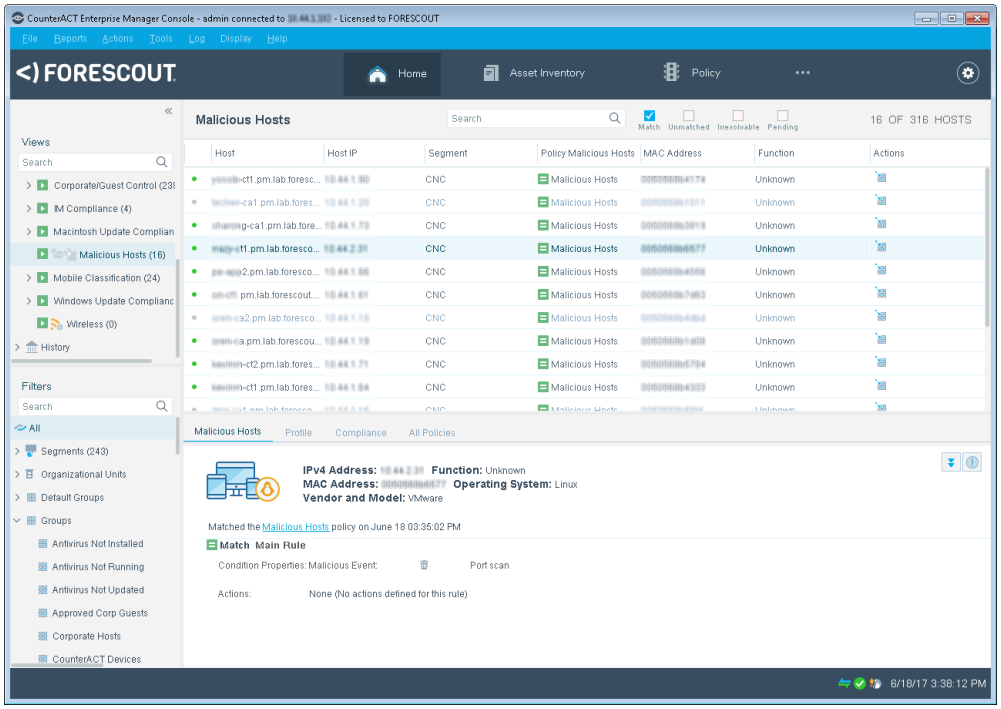
Evaluate Threats

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.



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.

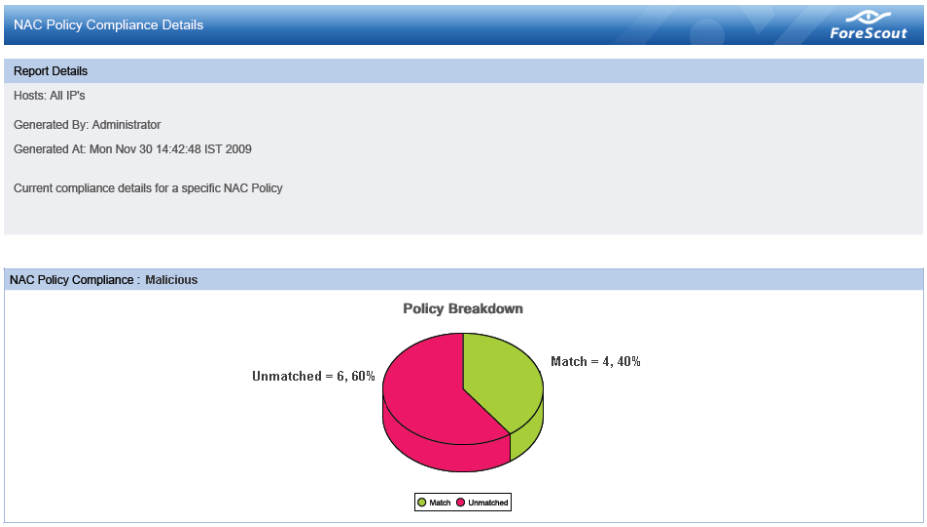
The Reports Portal provides tools to customize reports and schedule automatic report generation. For more information about this portal, see the Forescout Administration Guide*.*

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 network assets. It also provides details about each asset, 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).