Forescout

Manage External Devices

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 14:19

Table of Contents

About Managing External Devices

Forescout® provides powerful tools that let you quickly and continuously track and control external devices connected to your network hosts.

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

- Use a wizard-based policy template to detect and classify hosts that have any of the following external device types connected to them:

  - Wireless communication devices
  - Windows portable devices
  - Windows CE USB devices
  - Printers
  - PCMIA and flash memory devices
  - Other devices (devices that the Forescout platform cannot classify)
  - Network adapters
  - Modems
  - Infrared devices
  - Imaging devices
  - Disk drives
  - DVD/CD-ROM drives
  - Bluetooth radios

  Hosts are automatically organized into groups, based on the type of external device connected.

- Use Forescout tools to review an extensive range of information about each external device, the hosts connected to them, and the users who are logged into them.

- Generate real-time and trend reports that evaluate external device connections.

- 📄 *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. *See* Additional Forescout Documentation *for information on how to access this guide.*

Prerequisites

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

- Verify that the *Windows* group appears in the Console, Filters pane. If not, run the *Primary Classification* template policy to create this group. Refer to the *Forescout Administration Guide* for details.

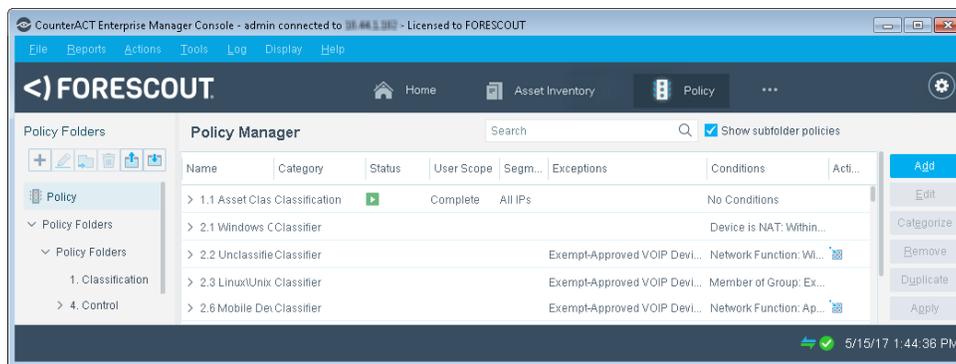# Create and Apply an External Device Classification Policy

Follow these steps to detect and classify external devices using a policy template:

- [Select the External Device Classification Template](#)
- [Choose Hosts to Inspect](#)
- [Choose Devices to Detect](#)
- [Activate the Policies](#)

## Select the External Device Classification Template

To select the External Device Classification template:

1. Log in to the Forescout Console.

2. Select the Policy tab. The Policy Manager opens.

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

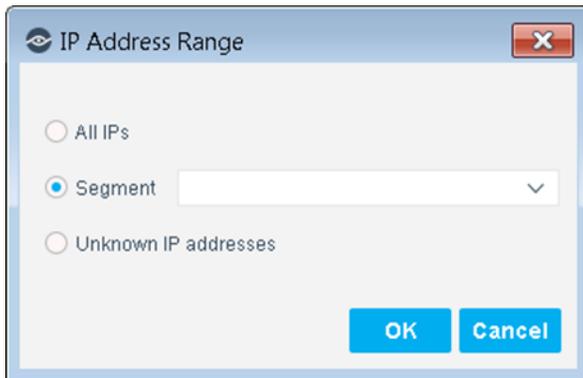4. Under **Templates**, expand the **Classification** folder and select **External Device Classification**.
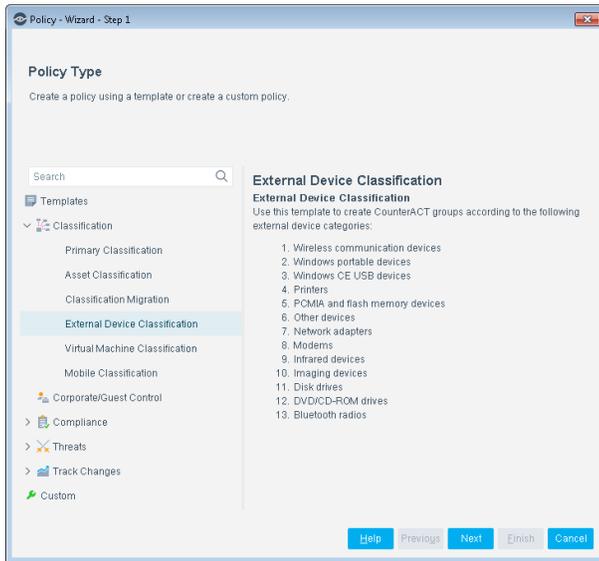
5. Select **Next**. The Scope pane and the IP Address Range dialog box open.

Choose Hosts to Inspect

To choose 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 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.

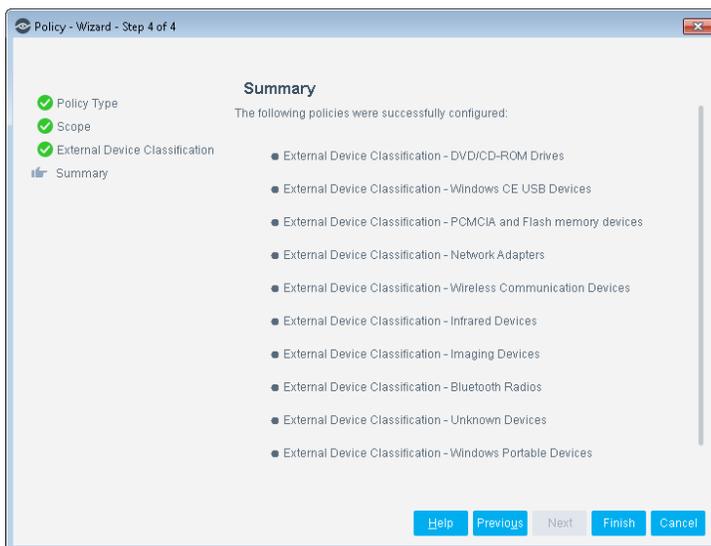**3.** Select **Next**. The External Device Classification pane opens.

Choose Devices to Detect

To choose devices to detect:

1. Select the external device types you want to detect, or select **Select All**.
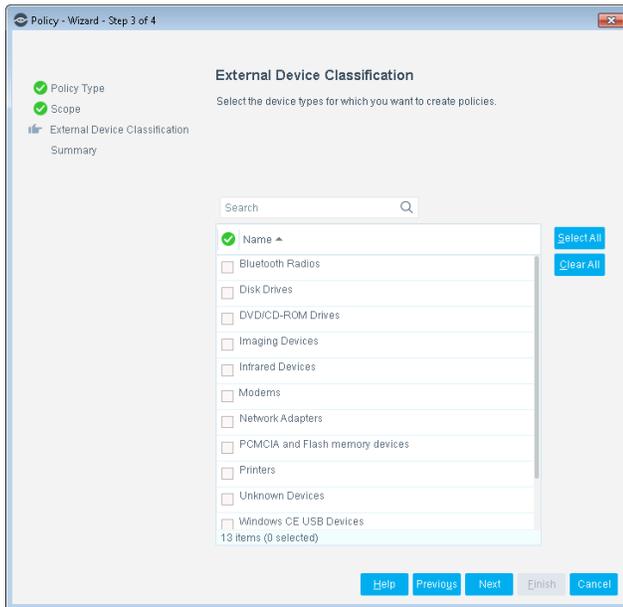
**2.** Select **Next**. The Summary pane opens.

The Summary pane provides a summary of the device types that you have instructed the Forescout platform to detect. A separate policy is created for each device type selected.

3. Select **Finish**. The policies automatically appear in the Policy Manager, where they can be activated.

Activate the Policies

To activate policies:

1. Select the Policy tab.

2. For each of the policies you created, perform the following:

    a. In the Policy Manager, select the policy.
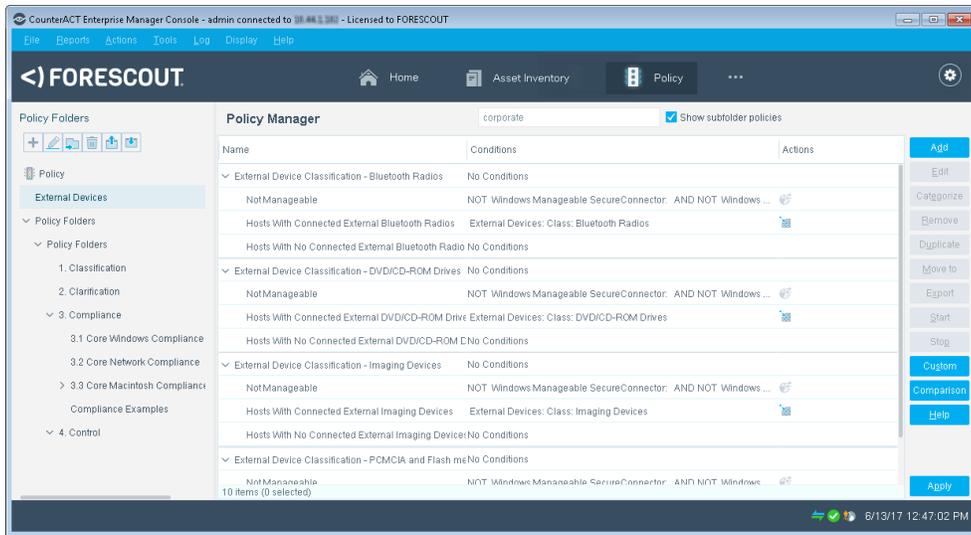
    b. Select **Apply**. The policy is activated. The Forescout platform detects external devices connected to the addresses you specified in the Scope pane, and adds the devices to the External Devices group.

3. Select the Home tab.

4. In the Filters pane, expand the **Groups** folder and scroll to view the External Devices group.
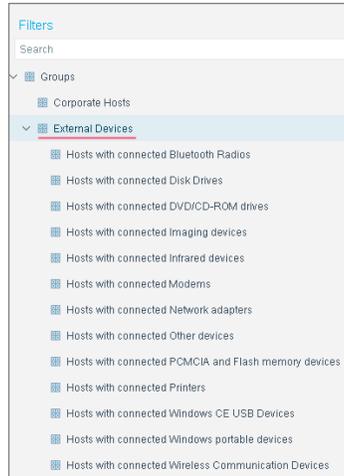
Evaluate External Device Information

After activating the policy, you can view an extensive range of details about external devices, as well as hosts and users connected to them.

To view details about external devices:

1. Select the Home tab.

2. Perform one of the following:

   – In the Views pane, expand the **Policy** folder and scroll to the External Devices policy.

   – In the Filters pane, expand the **Groups** folder and select the External Devices group.

3. In the Detections pane, select a host. Host information is displayed in the Details pane.

4. To customize the information displayed about external devices and users connected to external devices, 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 and users connected to external devices. 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 **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 Summaries report was selected. This report gives you a breakdown of hosts connected to external devices, and provides details about each host 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.

Manage External Devices   How-to Guide

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).