ForeScout CounterACT®

Manage External Devices

How-to Guide

Version 8.0

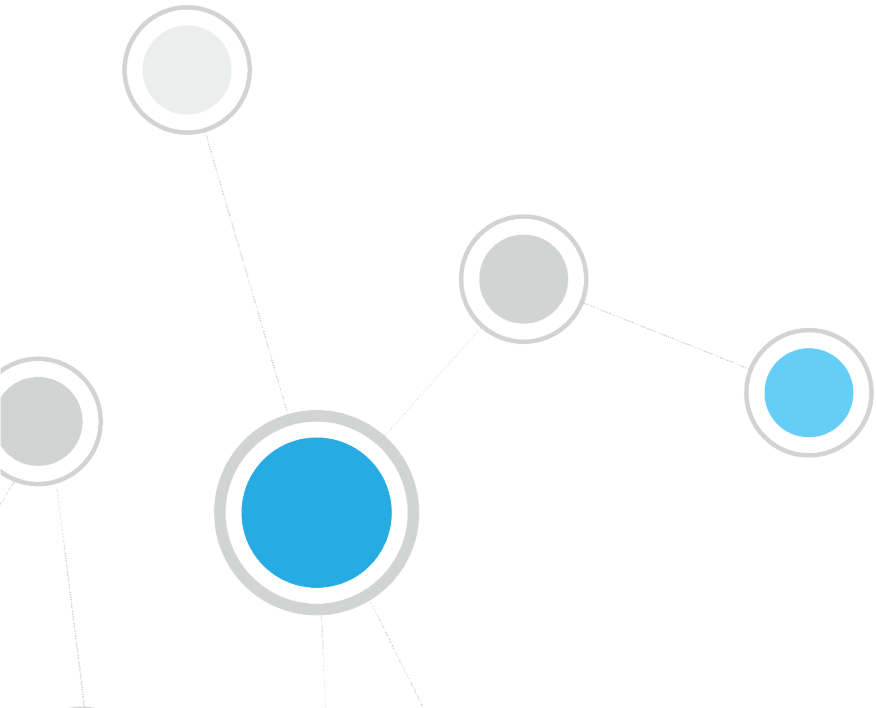


Table of Contents

About Managing External Devices

ForeScout CounterACT® 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 CounterACT 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 CounterACT 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 CounterACT Administration Guide. See Additional CounterACT Documentation for information on how to access this guide.

Prerequisites

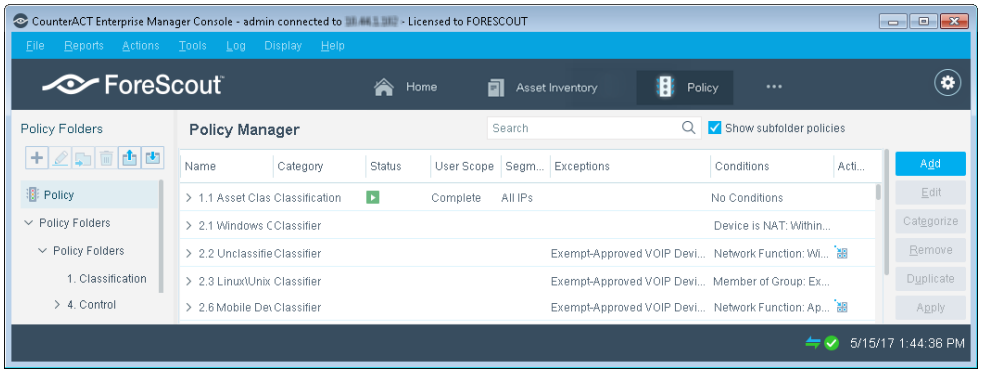
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the *CounterACT Administration Guide* for details.
- Verify that the *Windows* group appears in the Console, Filters pane. If not, run the *Asset Classification* template policy to create this group. Refer to the *CounterACT Administration Guide* for details.

Create and Apply an External Device Classification Policy

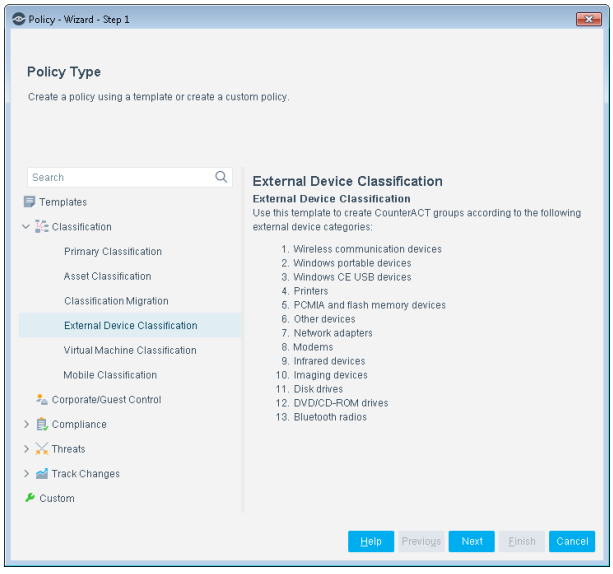
Follow these steps to detect and classify external devices using a policy template.

Select the External Device Classification Template

1. Log into the CounterACT Console.
2. Select the Policy tab. The Policy Manager opens.



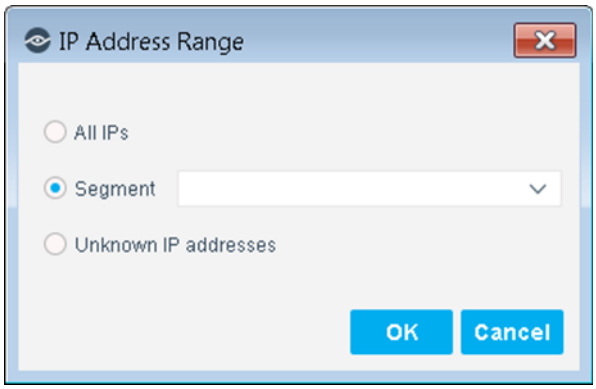
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Classification** folder and select **External Device Classification**.



5. Select **Next**. The Scope pane and the IP Address Range dialog box open.

Choose 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.

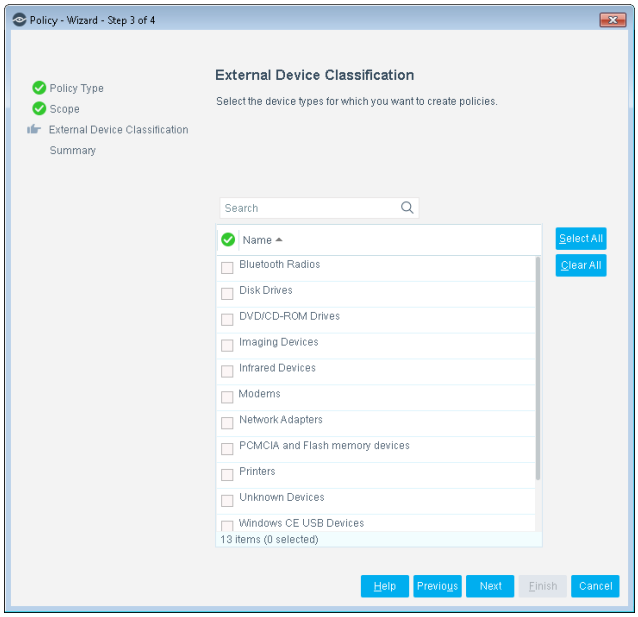
  Not applicable for this policy template.

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

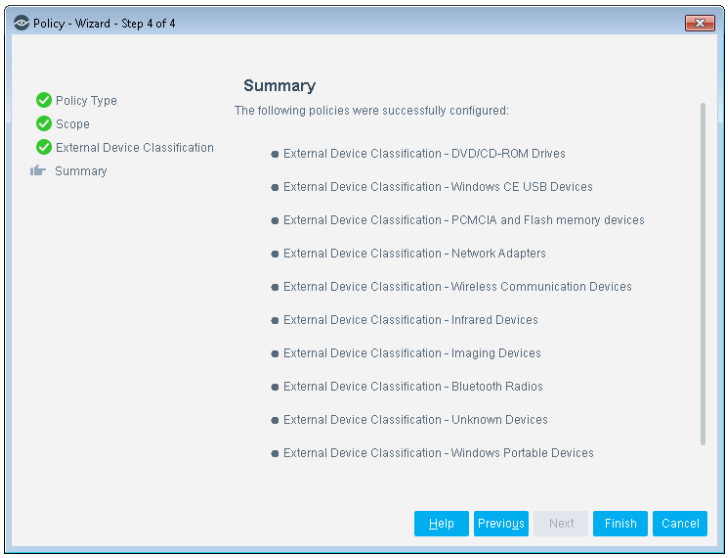
2. Select **OK**. The added range appears in the Scope list.
3. Select **Next**. The External Device Classification pane opens.

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.



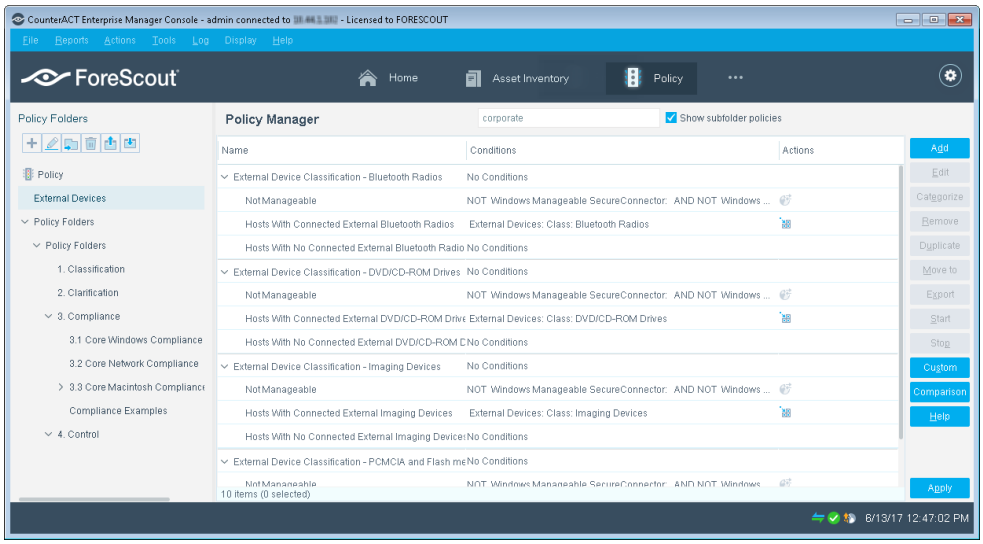
The Summary pane provides a summary of the device types that you have instructed CounterACT to detect. A separate policy is created for each device type selected.

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

4 Activate the Policies

1. Select the Policy tab.
2. For each of the policies you created, perform the following:

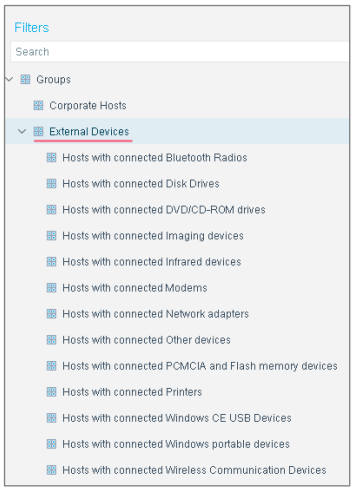
a. In the Policy Manager, select the policy.



b. Select **Apply**. The policy is activated. CounterACT 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.

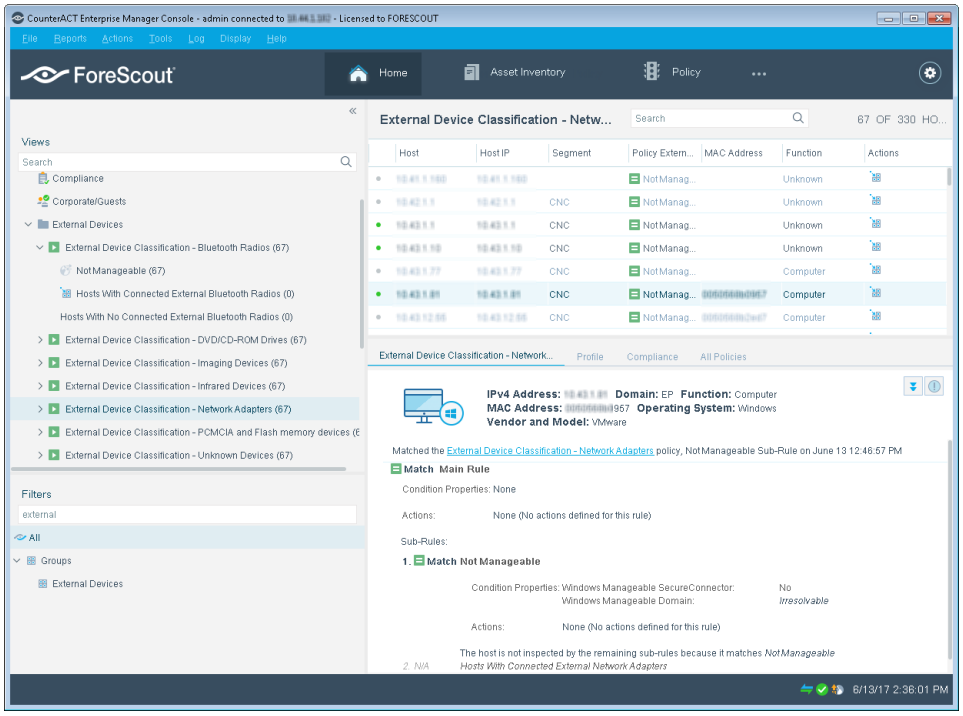


Evaluate External Device Information

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 CounterACT 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.

Policy Compliance Summaries

ForeScout

Report Details

Hosts: All IP's

Generated By: Administrator

Generated At: Mon Jun 08 18:32:33 IDT 2009

Current compliance summaries for all NAC Policies

NAC Policy Name	Match	Unmatch	Irresolvable
1.External Devices			
1.External Device Classifier - Bluetooth Radios	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External Bluetooth Radios	0	0	1351
Hosts With No Connected External Bluetooth Radios	0	0	0
1.External Device Classifier - Disk Drives	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External Disk Drives	0	0	1351
Hosts With No Connected External Disk Drives	0	0	0
1.External Device Classifier - DVD/CD-ROM drives	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External DVD/CD-ROM drives	0	0	1351
Hosts With No Connected External DVD/CD-ROM drives	0	0	0
1.External Device Classifier - Imaging devices	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External Imaging devices	0	0	1351
Hosts With No Connected External Imaging devices	0	0	0
1.External Device Classifier - Infrared devices	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External Infrared devices	0	0	1351
Hosts With No Connected External Infrared devices	0	0	0
1.External Device Classifier - Modems	1959	891	0
Not manageable	608	1351	0
Hosts With Connected External Modems	0	0	1351

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**.

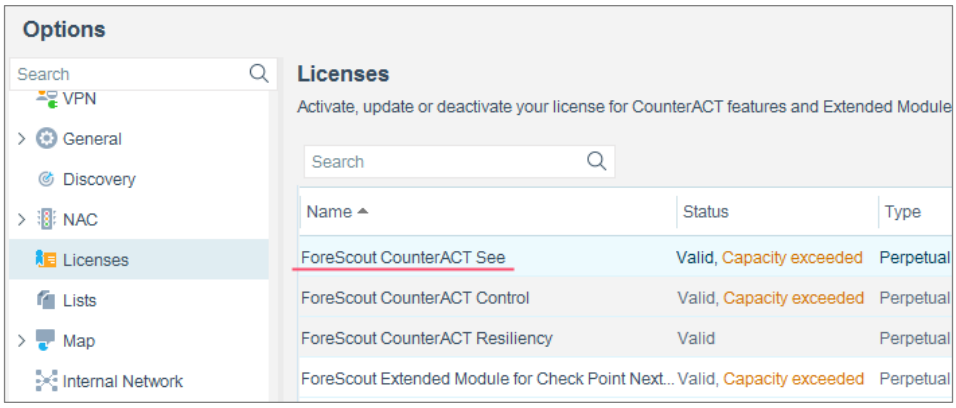
Documentation Portal

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.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-15 14:24