Manage External Devices
How-to Guide

CounterACT Version 7.0.0
# Table of Contents

About Managing External Devices

Prerequisites

Create and Apply an External Device Classification Policy

Evaluate External Device Information

Generate Reports
About Managing External Devices

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 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.

- 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 Console Online Help for details.
Create and Apply an External Device Classification Policy

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

1. **Select the External Device Classification 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 **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 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** 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 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.

Activate the Policies

1. On the Console toolbar, select the Policy tab.
2. For each of the policies you created, perform the following:
   a. In the Policy Manager, select the policy.
      
      ![Policy Manager screenshot]
      
      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. On the Console toolbar, select the NAC tab.
4. In the Filters pane, expand the **Groups** folder and scroll to view the External Devices group.

![Filters pane screenshot]

**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. On the Console toolbar, select the NAC 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** 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 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](image)

<table>
<thead>
<tr>
<th>NAC Policy Name</th>
<th>Match</th>
<th>Unmatched</th>
<th>Ineligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. External Device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· External Device Classifier - Bluetooth Radios</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External Bluetooth Radios</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External Bluetooth Radios</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2. External Device Classifier - Disk Drives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>· External Device Classifier - Disk Drives</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External Disk Drives</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External Disk Drives</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3. External Device Classifier - DVD/CD-ROM drives</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External DVD/CD-ROM drives</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External DVD/CD-ROM drives</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4. External Device Classifier - Imaging devices</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External Imaging devices</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External Imaging devices</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5. External Device Classifier - Unlicensed devices</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External Unlicensed devices</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External Unlicensed devices</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6. External Device Classifier - Modems</td>
<td>1399</td>
<td>891</td>
<td>2</td>
</tr>
<tr>
<td>· Hosts With Connected External Modems</td>
<td>0</td>
<td>0</td>
<td>1081</td>
</tr>
<tr>
<td>· Hosts With No Connected External Modems</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Legal Notice

Copyright © ForeScout Technologies, 2000-2015. All rights reserved.

The copyright and proprietary rights in this guide belong to ForeScout Technologies. It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this guide in any way, shape or form without the prior written consent of ForeScout Technologies.

This product is based on software developed by ForeScout Technologies. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004 and #8,639,800 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use, acknowledge that the software was developed by ForeScout Technologies.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All other trademarks used in this document are the property of their respective owners.

Send comments and questions about this document to: documentation@forescout.com

January 2015