Manage External Devices

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Managing External Devices 3
Prerequisites 3
Create and Apply an External Device Classification Policy 4
Evaluate External Device Information 7
Generate Reports 8

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

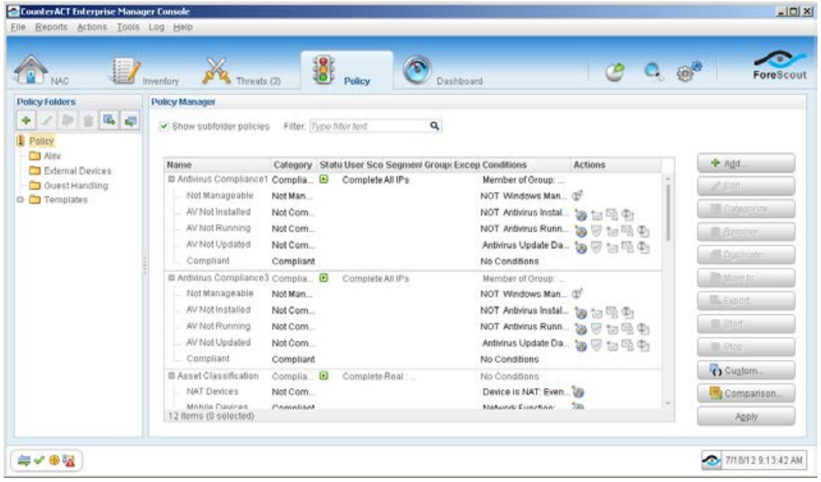
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.
- Verify that the *Windows* group appears in the Console, Filters pane. If not, run the *Asset Classification* template policy to create this group. Refer to the Console Online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

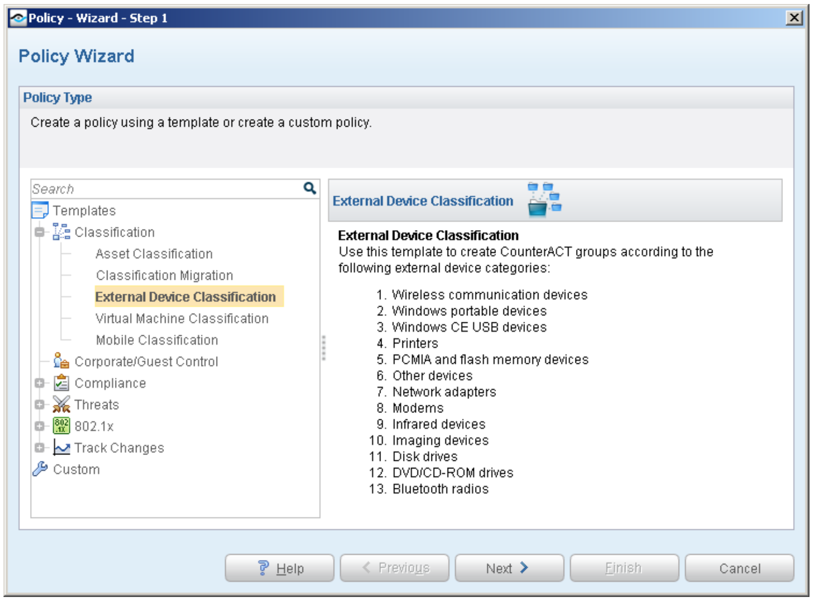


☑ Show subfolder policies Filter: Type filter text

Name	Category	Statu	User Sco	Segmen	Groups	Excep	Conditions	Actions
Antivirus Compliance1	Complia...	▶	Complete All IPs				Member of Group: ...	
Not Manageable	Not Man...						NOT Windows Man...	
AV Not Installed	Not Com...						NOT Antivirus Instal...	
AV Not Running	Not Com...						NOT Antivirus Runn...	
AV Not Updated	Not Com...						Antivirus Update Da...	
Compliant	Compliant						No Conditions	
Antivirus Compliance3	Complia...	▶	Complete All IPs				Member of Group: ...	
Not Manageable	Not Man...						NOT Windows Man...	
AV Not Installed	Not Com...						NOT Antivirus Instal...	
AV Not Running	Not Com...						NOT Antivirus Runn...	
AV Not Updated	Not Com...						Antivirus Update Da...	
Compliant	Compliant						No Conditions	
Asset Classification	Complia...	▶	Complete Real : ...				No Conditions	
NAT Devices	Not Com...						Device is NAT: Even...	
Mobile Devices	Compliant						Network Function: ...	

12 items (0 selected)

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**.



Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

External Device Classification

External Device Classification

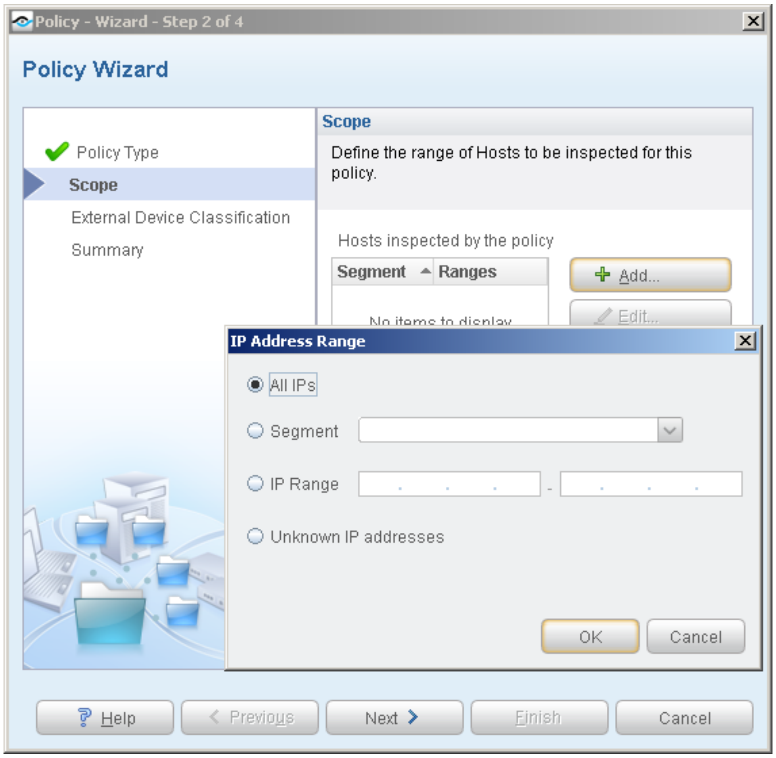
Use this template to create CounterACT groups according to the following external device categories:

1. Wireless communication devices
2. Windows portable devices
3. Windows CE USB devices
4. Printers
5. PCMIA and flash memory devices
6. Other devices
7. Network adapters
8. Modems
9. Infrared devices
10. Imaging devices
11. Disk drives
12. DVD/CD-ROM drives
13. Bluetooth radios

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

2 Choose the Hosts to Inspect

1. Use the IP Address Range dialog box to define the IP addresses you want to inspect.



Policy - Wizard - Step 2 of 4

Policy Wizard

✓ Policy Type
Scope
External Device Classification
Summary

Scope

Define the range of Hosts to be inspected for this policy.

Hosts inspected by the policy

Segment	Ranges
No items to display	

IP Address Range

● All IPs
○ Segment
○ IP Range
○ Unknown IP addresses

The following options are available:

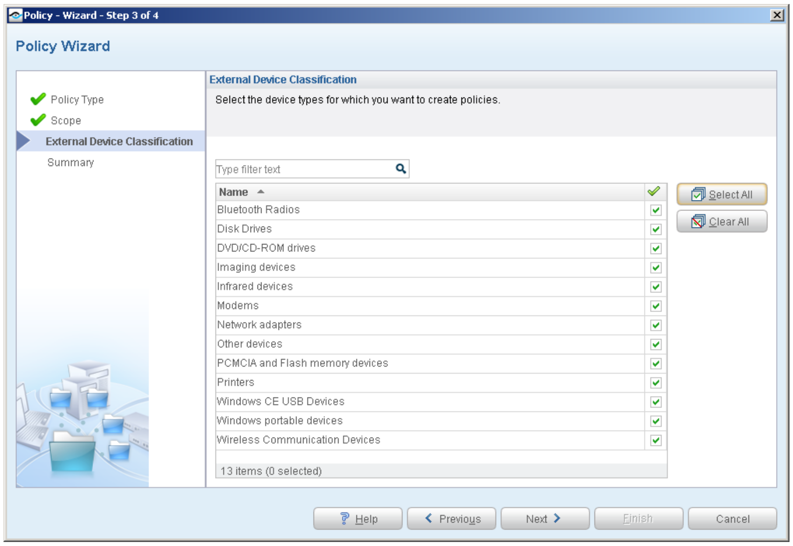
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments** 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**.



✓ Policy Type
✓ Scope
External Device Classification
Summary

External Device Classification

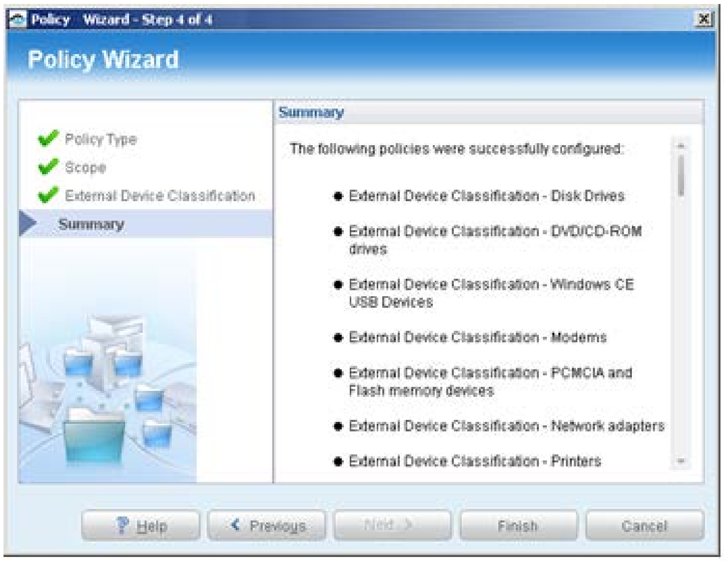
Select the device types for which you want to create policies.

Type filter text

Name	✓
Bluetooth Radios	☑
Disk Drives	☑
DVD/CD-ROM drives	☑
Imaging devices	☑
Infrared devices	☑
Modems	☑
Network adapters	☑
Other devices	☑
PCMCIA and Flash memory devices	☑
Printers	☑
Windows CE USB Devices	☑
Windows portable devices	☑
Wireless Communication Devices	☑

13 items (0 selected)

2. Select **Next**. The Summary pane opens.



✓ Policy Type
✓ Scope
✓ External Device Classification
Summary

Summary

The following policies were successfully configured:

- External Device Classification - Disk Drives
- External Device Classification - DVD/CD-ROM drives
- External Device Classification - Windows CE USB Devices
- External Device Classification - Modems
- External Device Classification - PCMCIA and Flash memory devices
- External Device Classification - Network adapters
- External Device Classification - Printers

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.

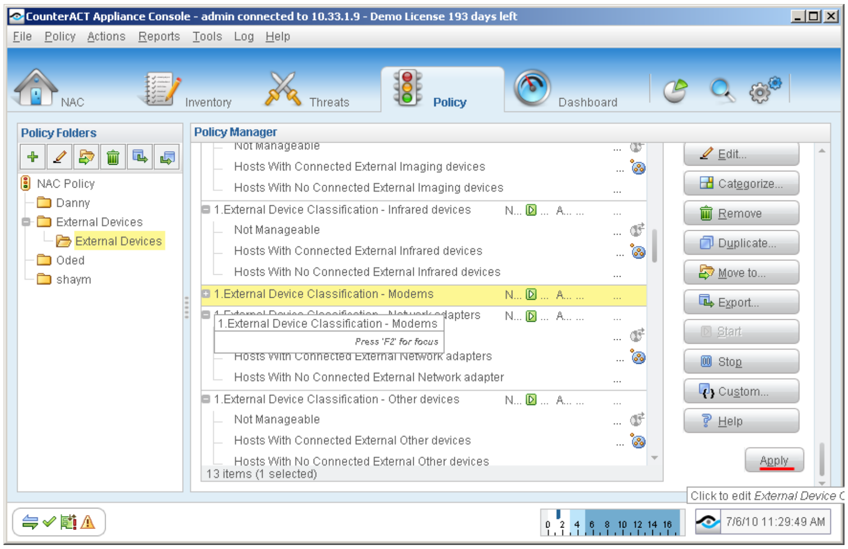
3. Select **Finish**. The policies automatically appear in the Policy Manager, where they can be activated.

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.



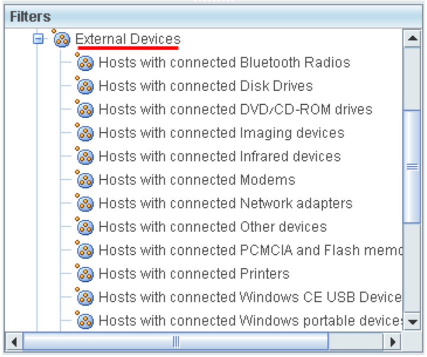
NAC Policy
- Danny
- External Devices
  - External Devices
- Oded
- shaym

Not Manageable
Hosts With Connected External Imaging devices
Hosts With No Connected External Imaging devices
1.External Device Classification - Infrared devices N... ... A... ...
Not Manageable
Hosts With Connected External Infrared devices
Hosts With No Connected External Infrared devices
1.External Device Classification - Modems N... ... A... ...
1.External Device Classification - Network adapters N... ... A... ...
1.External Device Classification - Modems
Press 'F2' for focus
Hosts With Connected External Network adapters
Hosts With No Connected External Network adapter
1.External Device Classification - Other devices N... ... A... ...
Not Manageable
Hosts With Connected External Other devices
Hosts With No Connected External Other devices
13 items (1 selected)

   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.



External Devices
- Hosts with connected Bluetooth Radios
- Hosts with connected Disk Drives
- Hosts with connected DVD/CD-ROM drives
- Hosts with connected Imaging devices
- Hosts with connected Infrared devices
- Hosts with connected Modems
- Hosts with connected Network adapters
- Hosts with connected Other devices
- Hosts with connected PCMCIA and Flash memo
- Hosts with connected Printers
- Hosts with connected Windows CE USB Device
- Hosts with connected Windows portable device

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.

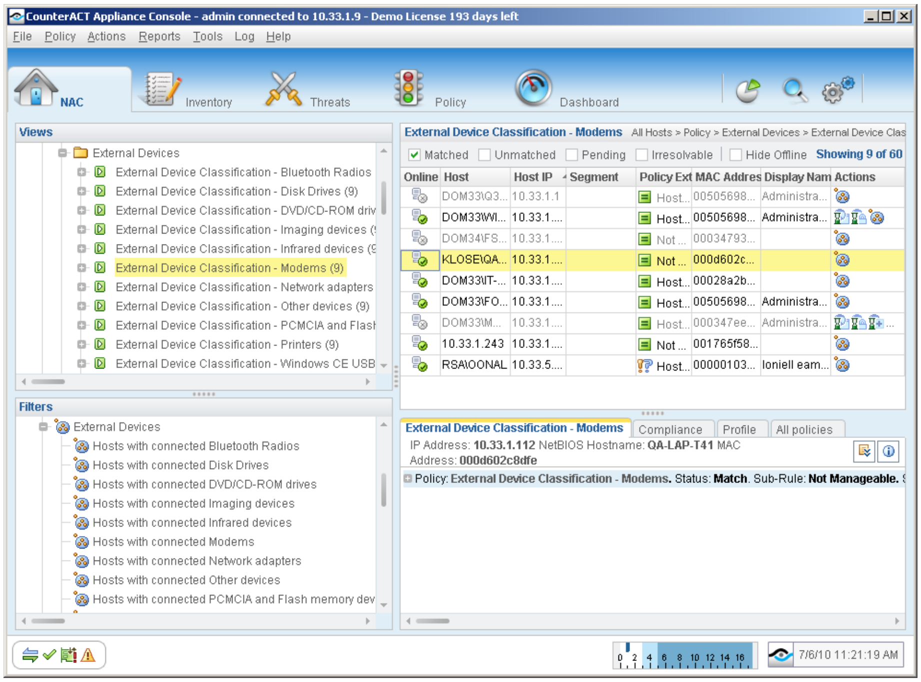
To view details about external devices:

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.



CounterACT Appliance Console - admin connected to 10.33.1.9 - Demo License 193 days left
File Policy Actions Reports Tools Log Help
NAC
Inventory
Threats
Policy
Dashboard

Views

- External Devices
  - External Device Classification - Bluetooth Radios
  - External Device Classification - Disk Drives (9)
  - External Device Classification - DVD/CD-ROM driv
  - External Device Classification - Imaging devices (
  - External Device Classification - Infrared devices (9
  - External Device Classification - Modems (9)
  - External Device Classification - Network adapters
  - External Device Classification - Other devices (9)
  - External Device Classification - PCMCIA and Flash
  - External Device Classification - Printers (9)
  - External Device Classification - Windows CE USB

Filters

- External Devices
  - Hosts with connected Bluetooth Radios
  - Hosts with connected Disk Drives
  - Hosts with connected DVD/CD-ROM drives
  - Hosts with connected Imaging devices
  - Hosts with connected Infrared devices
  - Hosts with connected Modems
  - Hosts with connected Network adapters
  - Hosts with connected Other devices
  - Hosts with connected PCMCIA and Flash memory dev

External Device Classification - Modems All Hosts > Policy > External Devices > External Device Clas

☑ Matched ☐ Unmatched ☐ Pending ☐ Irresolvable ☐ Hide Offline **Showing 9 of 60**

Online	Host	Host IP	Segment	Policy Ext	MAC Addres	Display Nam	Actions
	DOM33\Q3...	10.33.1.1		Host...	00505698...	Administra...	
✓	DOM33\WI...	10.33.1....		Host...	00505698...	Administra...	
	DOM34\FS...	10.33.1....		Not ...	00034793...		
✓	KLOSE\QA...	10.33.1....		Not ...	000d602c...		
✓	DOM33\IT-...	10.33.1....		Host...	00028a2b...		
✓	DOM33\FO...	10.33.1....		Host...	00505698...	Administra...	
	DOM33\M...	10.33.1....		Host...	000347ee...	Administra...	...
✓	10.33.1.243	10.33.1....		Not ...	001765f58...		
✓	RSA\OONAL	10.33.5....		Host...	00000103...	Ioniell eam...	

External Device Classification - Modems | Compliance | Profile | All policies

IP Address: **10.33.1.112** NetBIOS Hostname: **QA-LAP-T41** MAC Address: **000d602c8dfe**

Policy: **External Device Classification - Modems.** Status: **Match**. Sub-Rule: **Not Manageable.**

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.

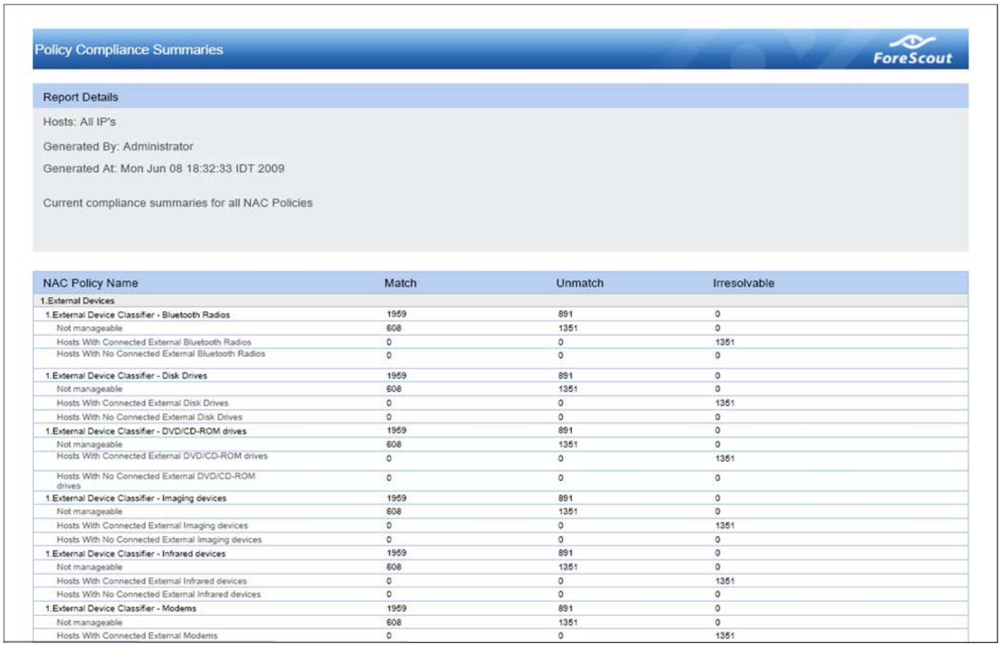
The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User Guide.

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

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

Legal Notice

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

January 2015