ForeScout

Classify Mobile Assets

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Mobile Device Classification

CounterACT provides powerful tools that let you continuously track and control your network mobile assets.

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

- Use a wizard-based CounterACT template to create a policy to classify mobile assets in your network into the following groups:
  - iOS
  - Kindle Fire
  - Android
  - Kindle
  - Windows Mobile
  - Blackberry
  - Symbian
  - Palm
  - Other
- Review an extensive range of information about each device, including IP, MAC Address, vendor, model, OS version, user directory information, and more.
- Generate real-time and trend reports about mobile assets.

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

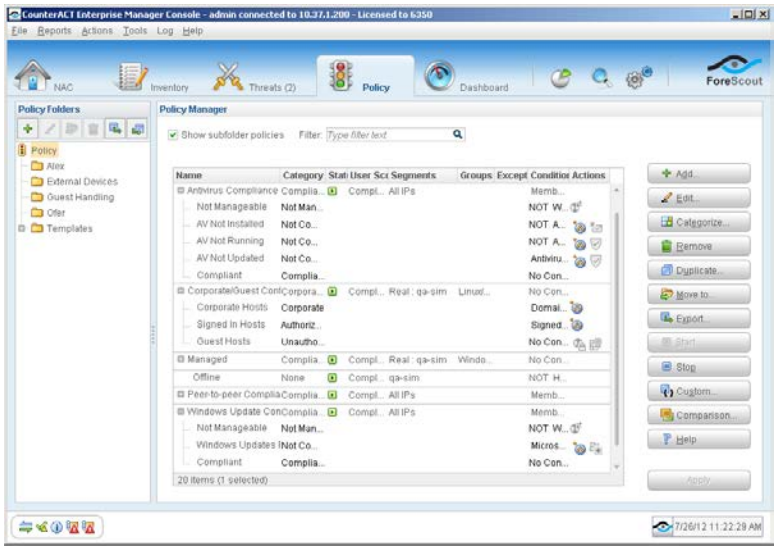
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.
- Verify that the *Mobile or Hand held* group appears in the Console, Filters pane. These groups are used by this policy template to further classify mobile devices. If one of these groups does not appear, run the *Asset Classification* template policy to create them and other asset groups. Refer to the Console Online Help for details.

Create a Mobile Classification Policy

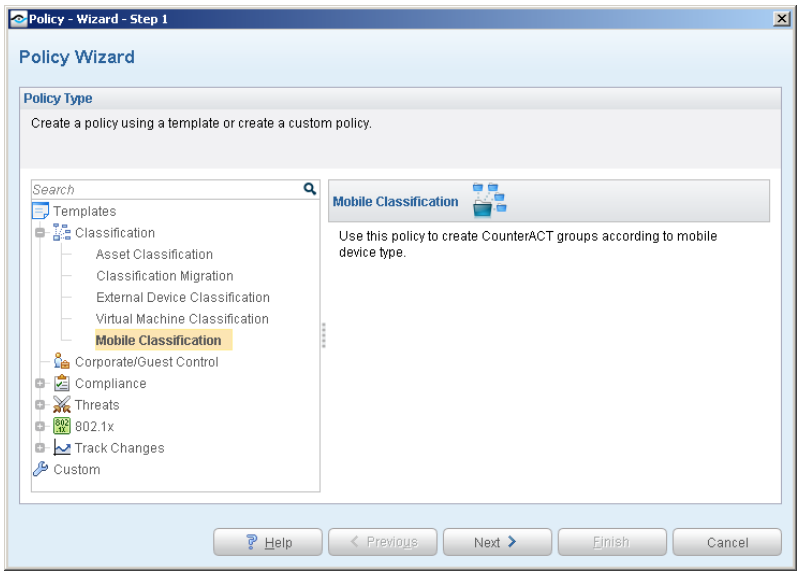
Follow these steps to detect and classify your network's mobile assets using a policy template.

Select the Mobile Classification Template

1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



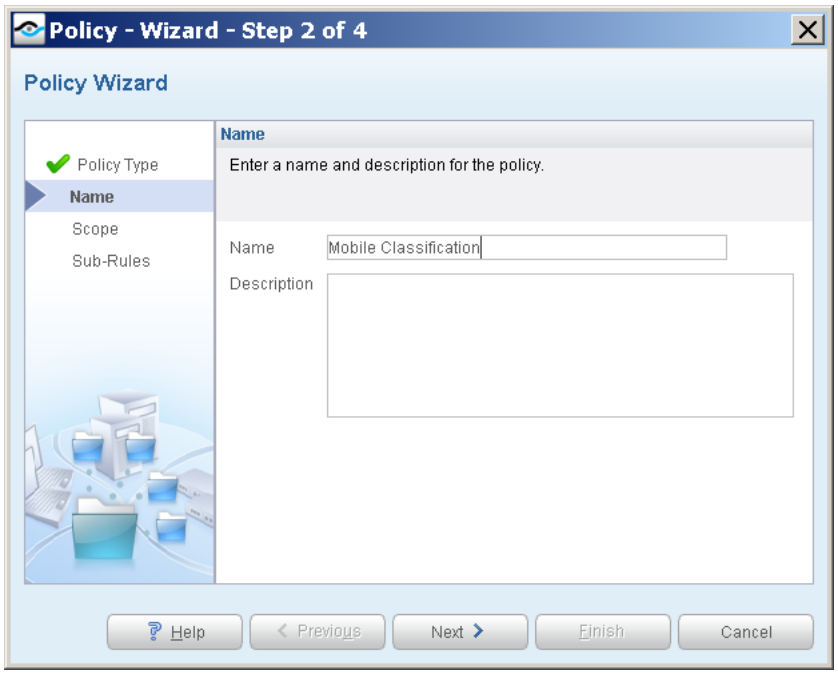
3. In the Policy Manager pane select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Classification** folder and select **Mobile Classification**.



5. Select **Next**. The Name pane opens.

2 Name the Policy

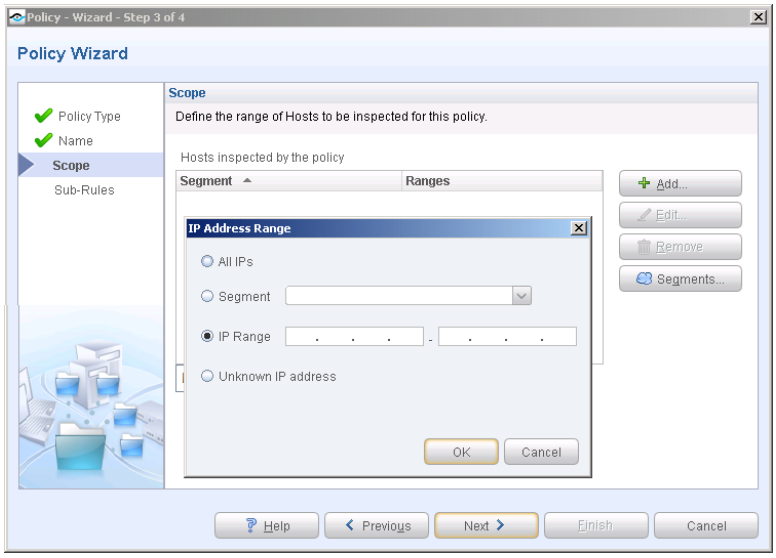
1. In the Name pane, a default policy name appears in the **Name** field.



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 open.

Choose the Hosts to Inspect

1. Use the IP Address Range dialog box to specify the hosts you want to inspect.



The following options are available:

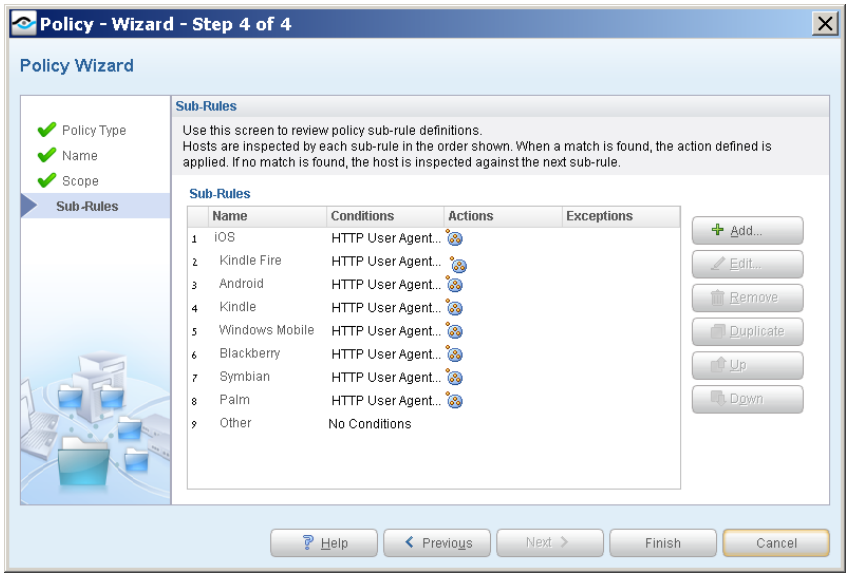
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments**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

Finish Policy Creation

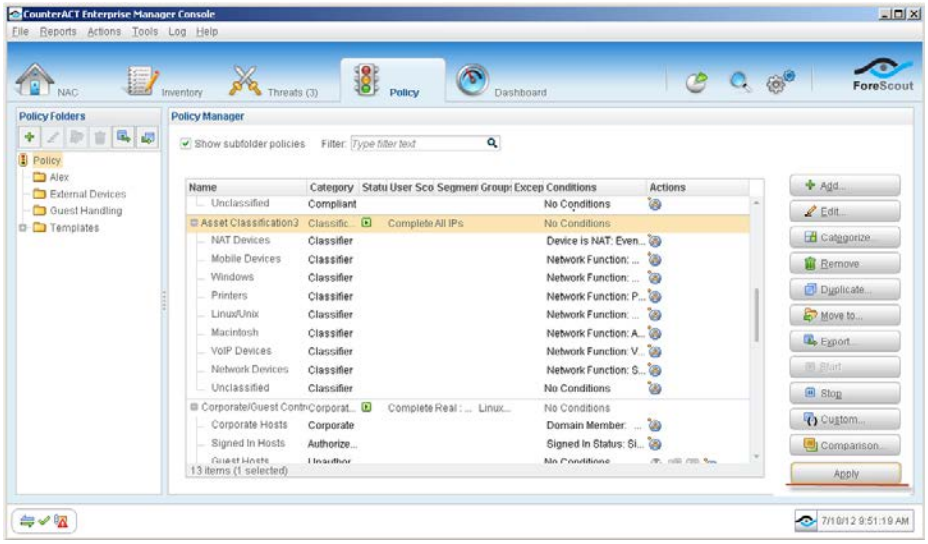
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). All actions are defined by default to sort all of your assets into their respective device groups.



1. Select Finish. The policy automatically appears highlighted in the Policy Manager, where it can be activated.

5 Activate the Policy

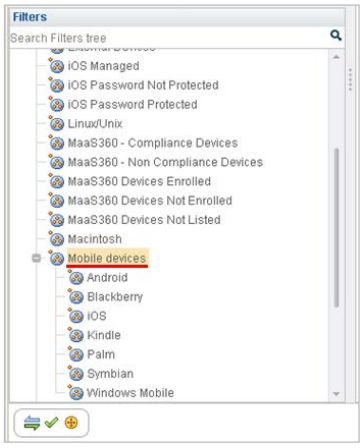
1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, select the policy you created.



3. Select **Apply**. The policy is activated.

   CounterACT detects mobile assets at the addresses you specified in the Scope pane, and adds the assets to their appropriate groups.
4. On the Console toolbar, select the NAC tab.

5. In the Filters pane, expand the **Groups** folder and scroll to view the groups.

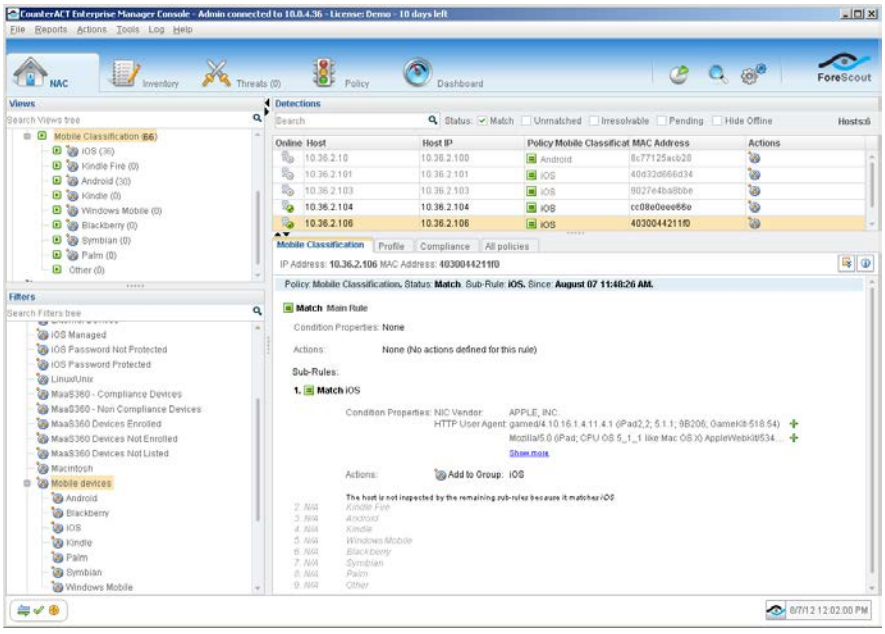


Evaluate Mobile Assets

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

To evaluate mobile devices:

1. On the Console toolbar, select the NAC tab.
2. In the Views pane, expand the **Policy** folder and select the Mobile policy containing your mobile asset classification policy.
3. In the Detections pane, select a host. Host information is displayed in the Details pane.



4. To customize the information displayed about mobile 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

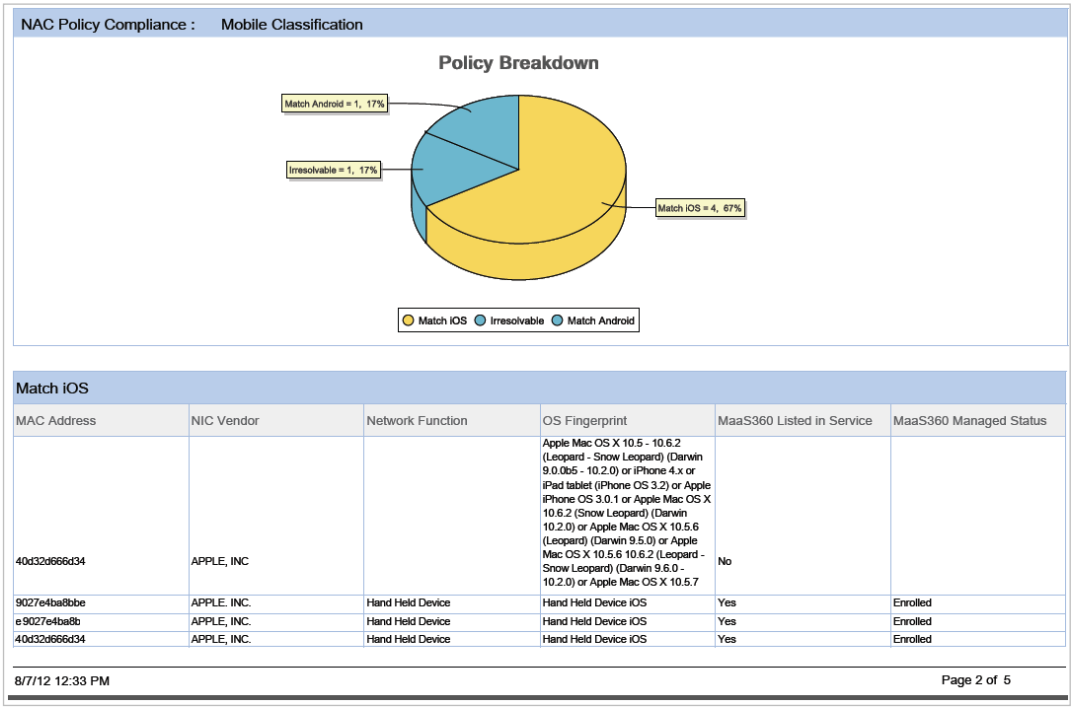
After the policy runs, you can generate reports with real-time and trend information about your network assets. You can generate and view the reports immediately, or generate schedules to ensure that your assets are automatically and consistently reported.

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 NAC Policy Compliance report was selected.



NAC Policy Compliance : Mobile Classification

Policy Breakdown

Match iOS

MAC Address	NIC Vendor	Network Function	OS Fingerprint	MaaS360 Listed in Service	MaaS360 Managed Status
40d32d666d34	APPLE, INC		Apple Mac OS X 10.5 - 10.6.2 (Leopard - Snow Leopard) (Darwin 9.0.0b5 - 10.2.0) or iPhone 4.x or iPad tablet (iPhone OS 3.2) or Apple iPhone OS 3.0.1 or Apple Mac OS X 10.6.2 (Snow Leopard) (Darwin 10.2.0) or Apple Mac OS X 10.5.6 (Leopard) (Darwin 9.5.0) or Apple Mac OS X 10.5.6 10.6.2 (Leopard - Snow Leopard) (Darwin 9.6.0 - 10.2.0) or Apple Mac OS X 10.5.7	No	
9027e4ba8bbe	APPLE, INC.	Hand Held Device	Hand Held Device iOS	Yes	Enrolled
e9027e4ba8b	APPLE, INC.	Hand Held Device	Hand Held Device iOS	Yes	Enrolled
40d32d666d34	APPLE, INC.	Hand Held Device	Hand Held Device iOS	Yes	Enrolled

8/7/12 12:33 PM Page 2 of 5

Classification Tips

To ensure that all mobile devices are identified, you may need to fine-tune the conditions in the Mobile Classification template or the Asset Classification template as follows:

- By default, CounterACT must detect HTTP traffic (browsing) on the device to classify it. Alternatively, you can add the *NIC Vendor* condition to device sub-rules, with the names of mobile NIC vendors. The devices are detected based on the vendor name, without the need to wait for browsing. For example, if you add the *RIM, NIC Vendor* condition to your *Asset Classification> Hand Held Devices* sub-rule, the BlackBerry devices will be classified based on the vendor name.
- Mobile devices are detected when the access point is configured as a bridge. By default, the template does not detect mobile devices when their access point is configured as a gateway or router. You can use the *Device is NAT* condition to detect mobile devices that use gateway or router access points.

Legal Notice

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

January 2015