ForeScout

Classify Assets

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Asset Classification

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

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

- Use a wizard-based policy template to classify your network into the following asset groups:
  - Network Address Translation (NAT) devices
  - Mobile devices
  - Windows devices
  - Printers
  - Linux/Unix devices
  - Macintosh devices
  - VoIP devices
  - Network devices such as routers and switches
  - Unclassified devices
- Use CounterACT tools to review an extensive range of information about each device and about the users connected to them.
- Generate real-time and trend reports about network assets.

It is recommended to run the Asset Classification template before running any other policy template. Asset Classification groups are used when working with other templates. Organizing your network hosts into asset groups makes it easier to create and manage other policies and track policy results.

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

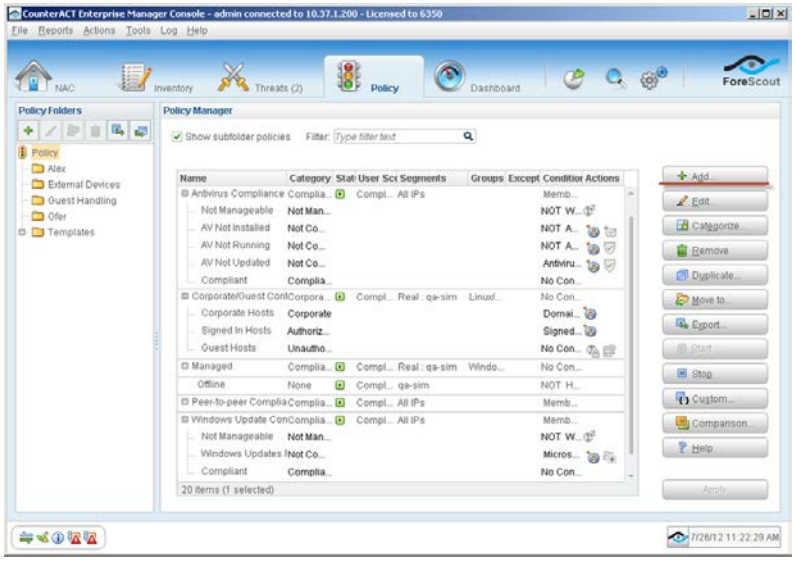
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.

Create an Asset Classification Policy

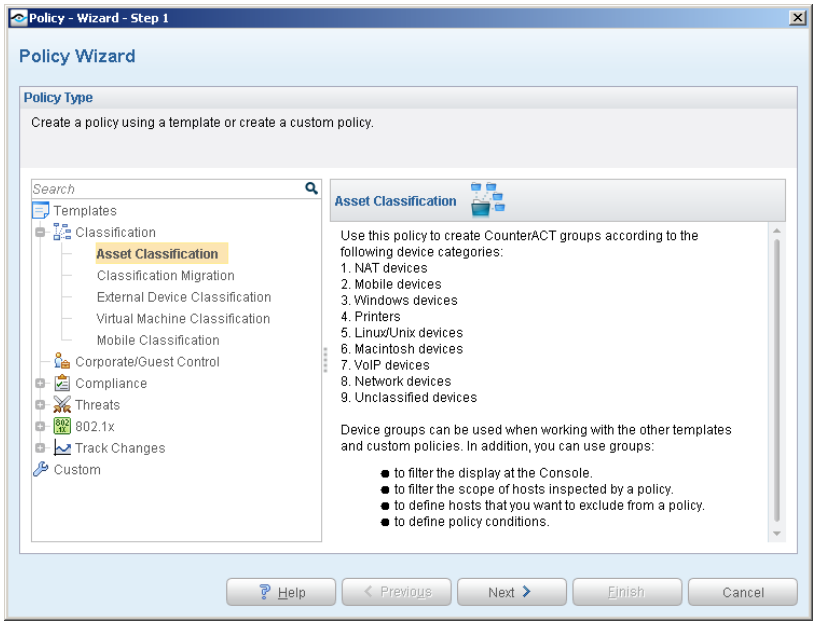
Follow these steps to detect and classify your network assets using a policy template.

Select the Asset Classification Template

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



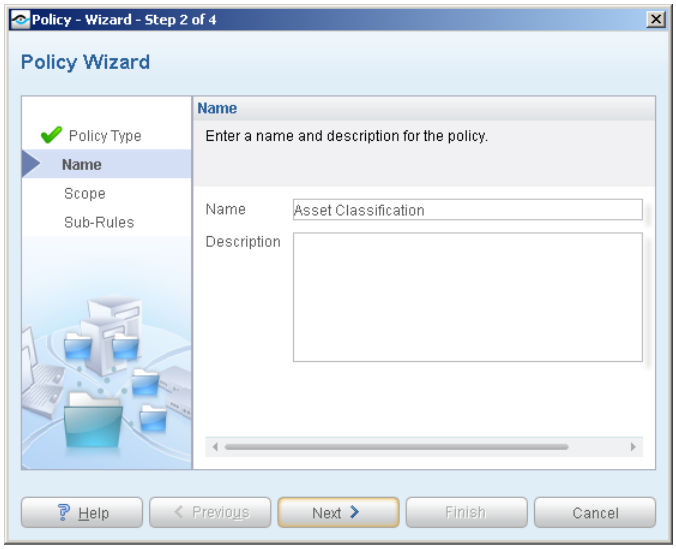
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Classification** folder and select **Asset Classification**.



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

2 Name the Policy

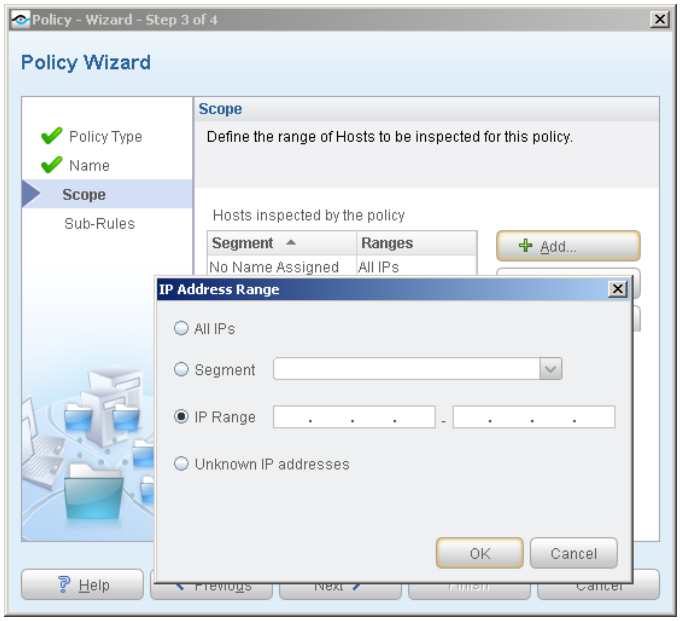
1. In the Name pane, a default policy name appears in the **Name** field.



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.

3 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:

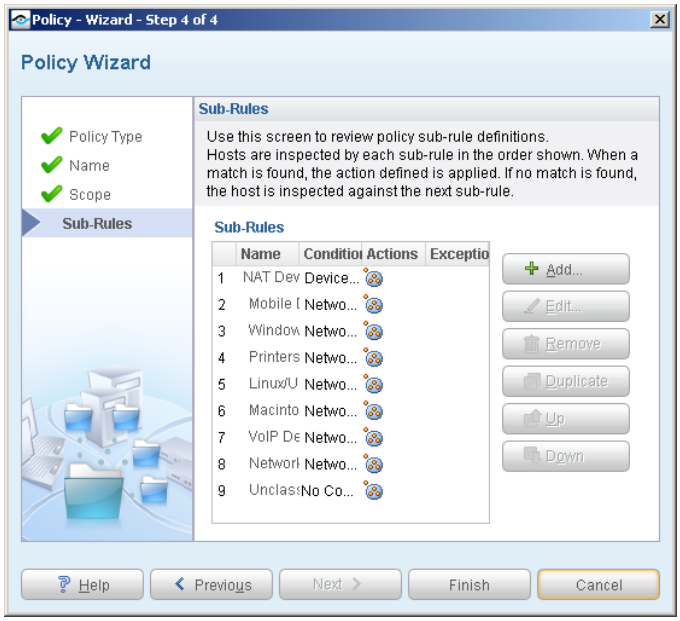
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments**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

4 Finish Policy Creation

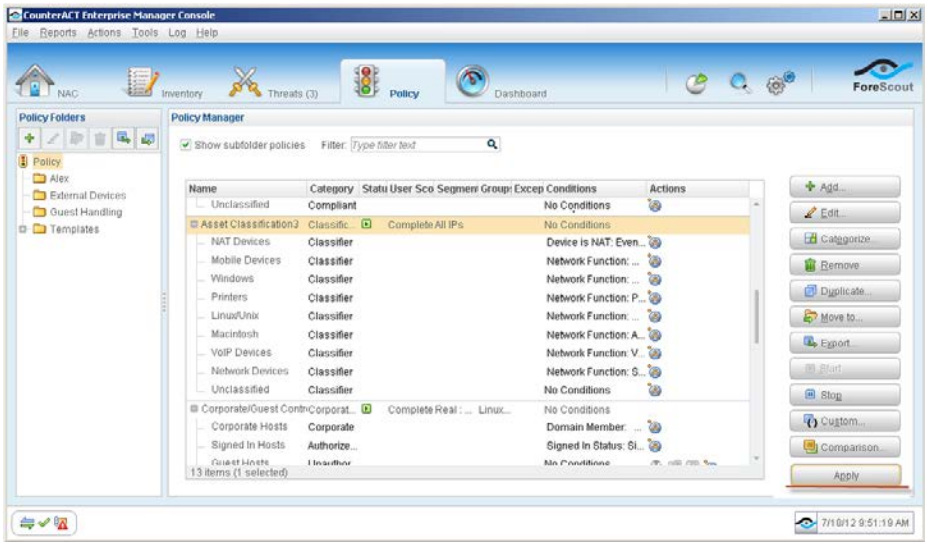
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). All actions are defined by default to sort all of your assets into their respective device groups.



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

5 Activate the Policy

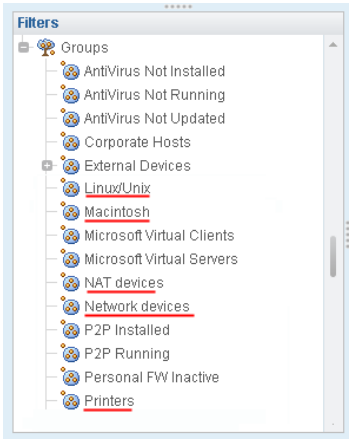
1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, select the policy you created.



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

   CounterACT detects assets at the addresses you specified in the Scope pane, and adds 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.

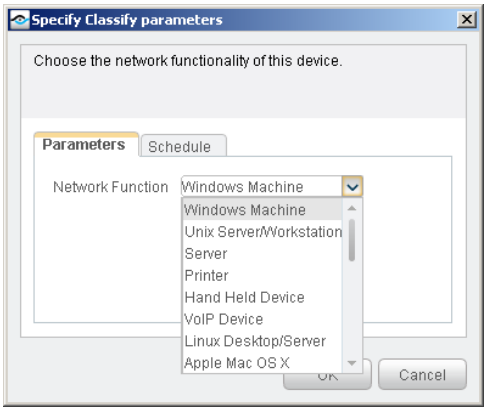


Fine-Tune Asset Classification

After you run the wizard, you can manually fine-tune asset classification. You can move an asset from a specific group to another, and you can classify an asset that was added to the Unclassified group by adding it to a specific group.

To re-classify an asset:

1. On the Console toolbar, select the NAC tab.
2. In the Views pane, expand the **Policy** folder and select the policy containing your asset classification policy.
3. In the Detections pane, right-click the asset to re-classify, and select **Manage>Classify**. The Specify Classify Parameters dialog box opens.



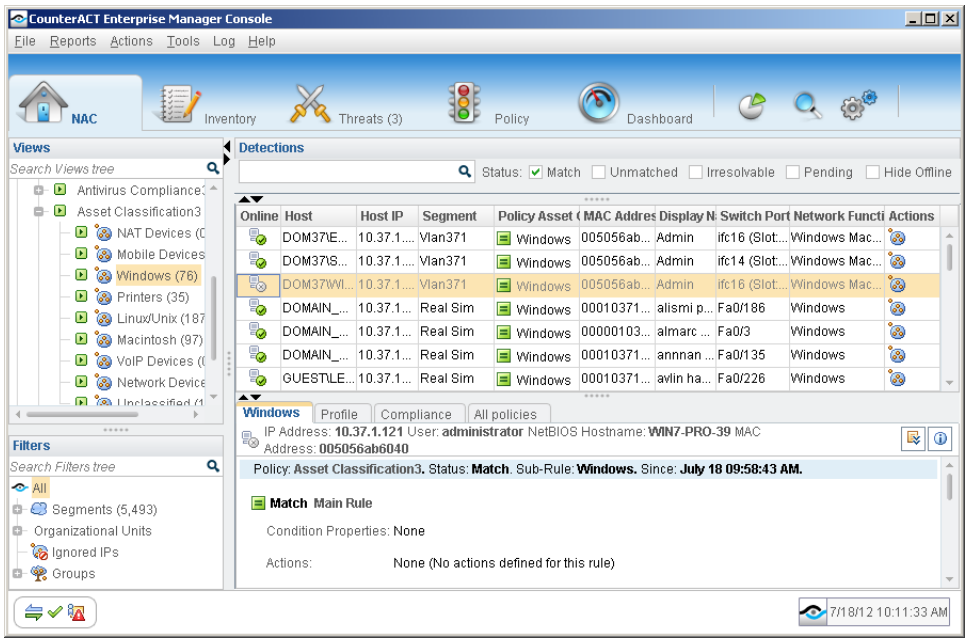
4. In the Parameters tab, select a network function from the drop-down list.
5. Select **OK**. The asset is re-classified.

Evaluate Assets

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

To evaluate assets:

1. On the Console toolbar, select the NAC tab.
2. In the Views pane, expand the **Policy** folder and select the policy containing your 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 hosts and users connected to assets, 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.

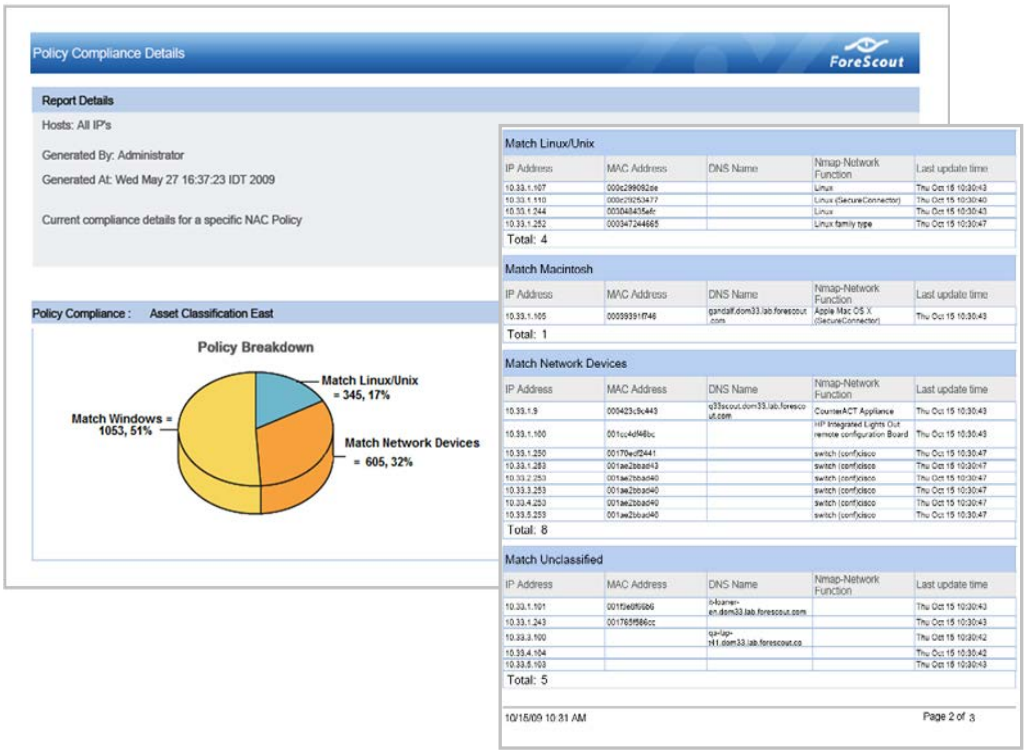
The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User Guide.

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 Policy Compliance Details report was selected. This report gives you a pie chart breakdown of network assets, and provides details about each asset depending on the information fields you selected to view.



Legal Notice

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

January 2015