ForeScout

Control Network Vulnerabilities

How-to Guide

CounterACT Version 7.0.0

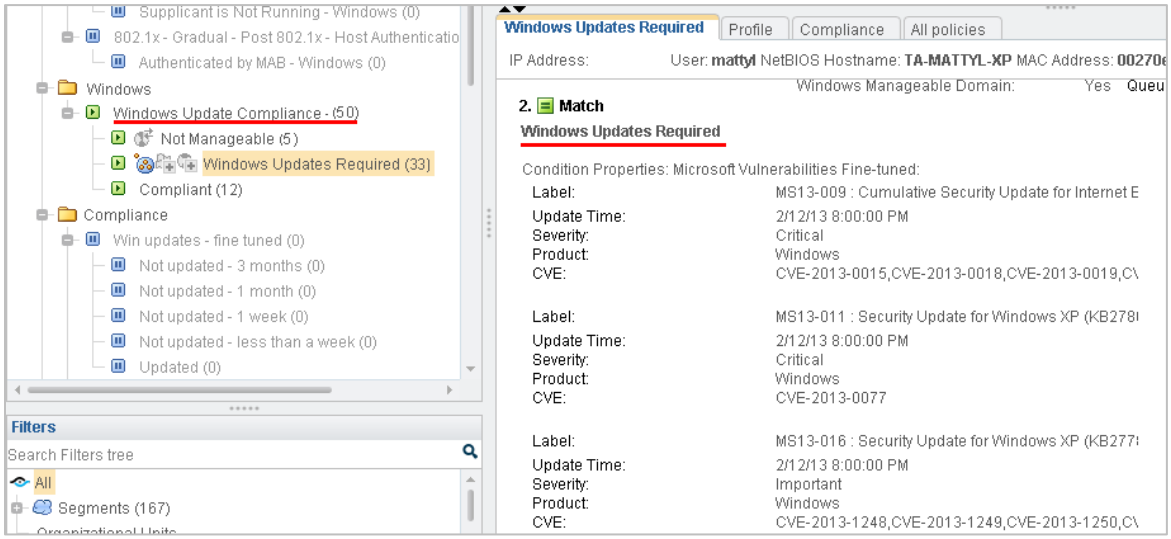
Table of Contents

About Controlling Network Vulnerabilities

CounterACT provides powerful tools that let you continuously detect, remediate and report Microsoft® OS and Office published vulnerabilities, and Macintosh vulnerabilities.

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

- Use a wizard-based CounterACT template to detect and remediate vulnerable endpoints.
- Review an extensive range of information about each device and about the users connected to them.
- Generate real-time and trend reports about vulnerable endpoints.



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

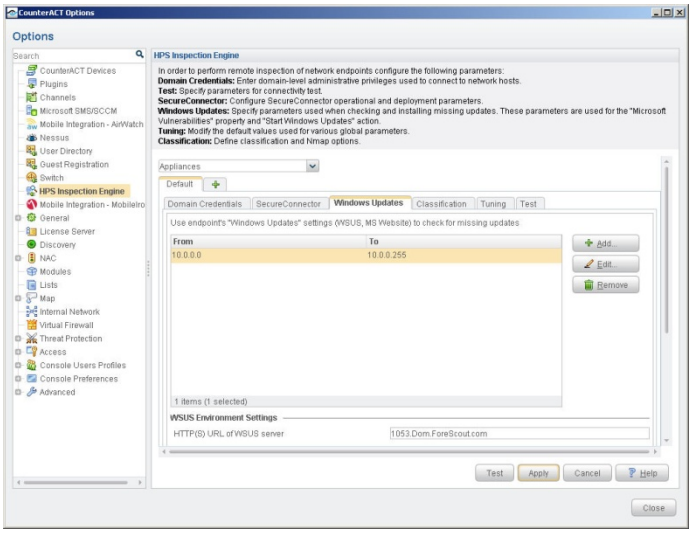
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.
- Verify that Windows and Macintosh groups appear in the Console, NAC view, Filters pane. If not, run the Asset Classification template policy to create these groups.
- If you are using an HTTP proxy to access the Internet, verify that the HPS Inspection Engine plugin is configured to access the Internet for updates. Refer to the Console Online Help for details.

Creating a Policy for Microsoft Vulnerabilities

Use CounterACT policies to detect Microsoft vulnerabilities at specific hosts or across your network. You can choose from the following methods to update non-compliant hosts with the latest Microsoft vulnerability updates:

- ***Automatic remediation***: CounterACT automatically updates hosts with the latest Microsoft vulnerability patches.

  Use the Microsoft web site or the Microsoft WSUS server to perform remediation according to a schedule that you set. To define WSUS server settings, select **Tools > Options > HPS Inspection Engine > Windows Updates** tab.



- ***Self-remediation***: CounterACT instructs users to update hosts with the latest Microsoft patches according to a preset schedule. You can include links to the Microsoft web site where users must download the latest vulnerability patches before they can continue to work.

Create a policy that detects vulnerabilities across your network. This policy allows you to:

- Detect hosts that have not been updated with the latest Microsoft-published vulnerability patches.
- Create a CounterACT *Windows Not Updated* group.

Optional remediation actions are disabled by default. Enable them to:

- Allow endpoint users to remediate from the desktop.
- Allow automatic remediation.

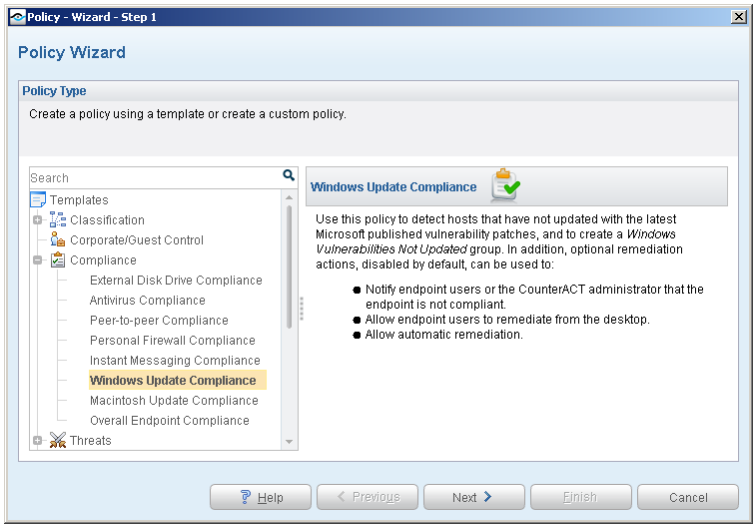
Remediation is performed from the Microsoft web site.

Endpoints must be managed by CounterACT, either by SecureConnector or remotely. There is an optional action, disabled by default, to install SecureConnector on unmanageable hosts.

Endpoints waiting for a reboot following the installation of a previous patch are not updated until after the reboot.

Create a Policy for Microsoft Vulnerabilities

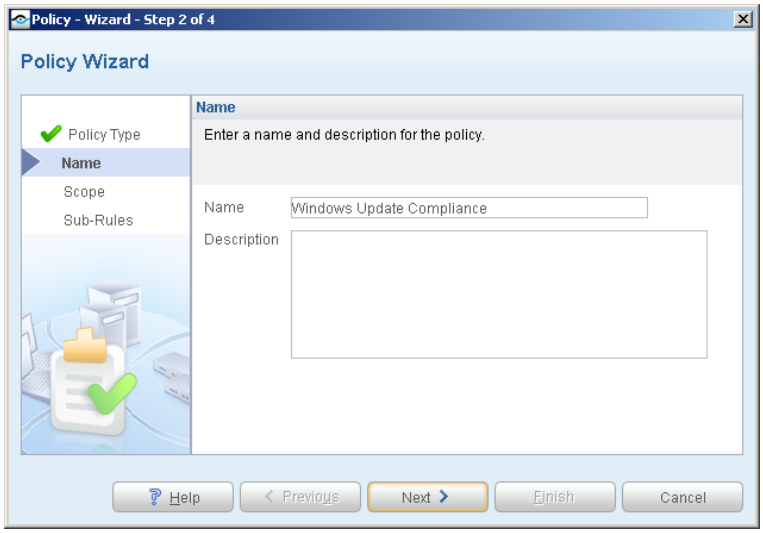
1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Windows Update Compliance**.



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

Name the Policy

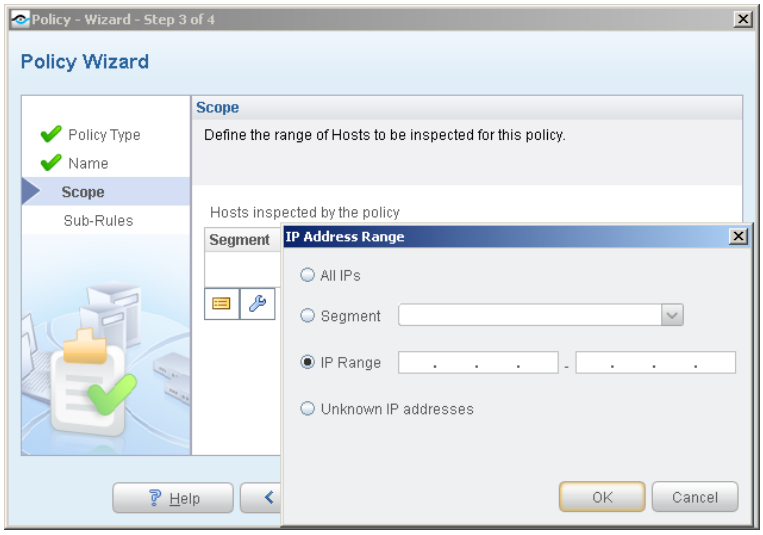
1. In the Name pane, a default policy name appears in the **Name** field.



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 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:

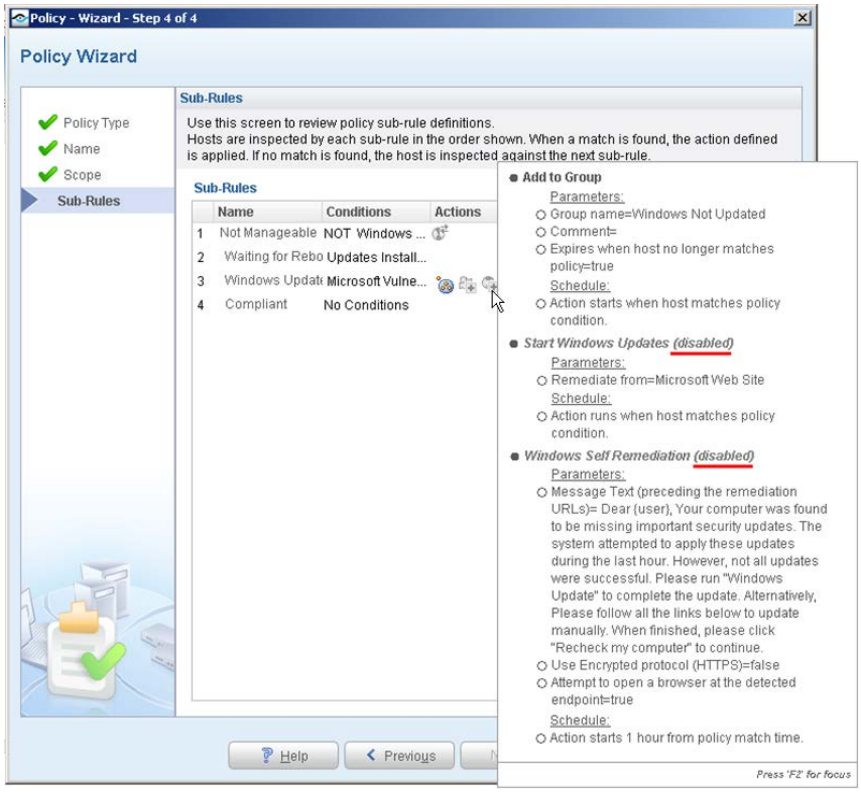
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments**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

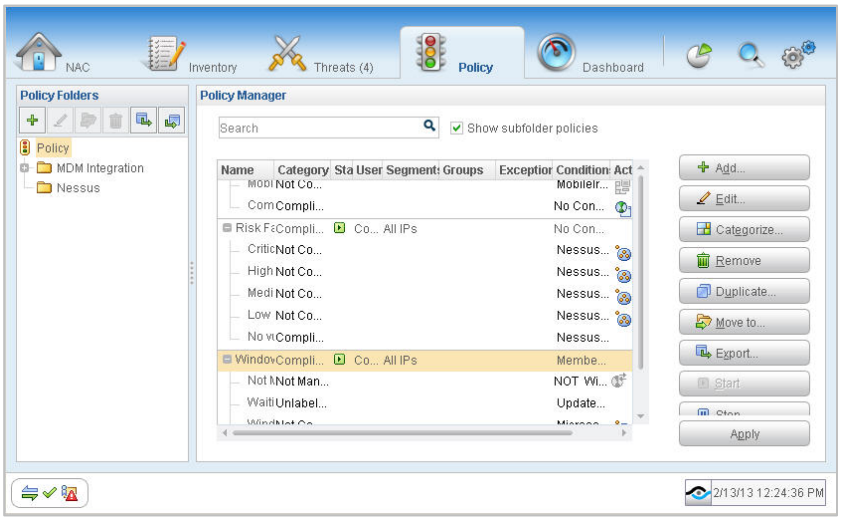
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). The *Add to Group* action is enabled by default. Optional remediation actions, disabled by default, can be used to start SecureConnector, start Windows Updates, and start Windows self-remediation. After you have run the policy and verified that results accurately reflect your network, you can remediate by enabling these actions.



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**.
4. A series of confirmation and completion dialog boxes opens. Select **Yes** or **OK** accordingly. On completion the policy is activated.

Creating a Policy for Macintosh Vulnerabilities

Use CounterACT policies to detect hosts that have not updated with the latest Macintosh published patches. Optional remediation actions, disabled by default, can be used to:

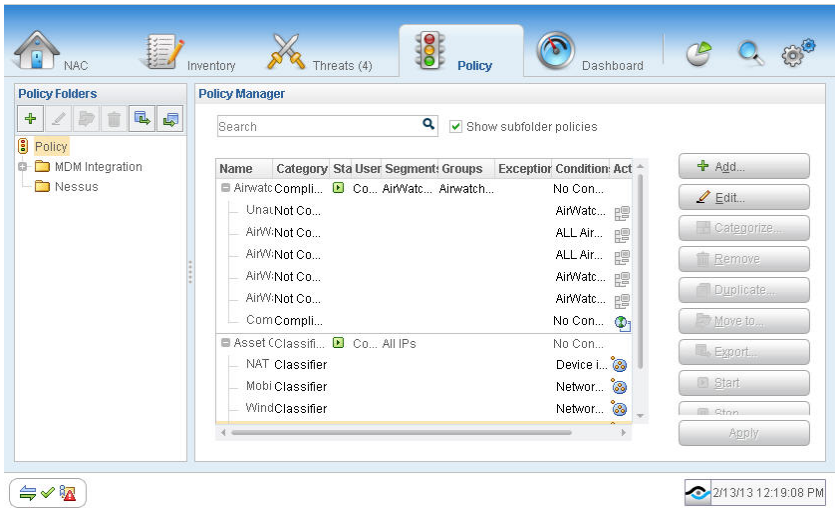
- Set up CounterACT to automatically provide the endpoints with appropriate patches for the missing Macintosh updates.
- Send an email message to a predefined user. The messages are sent according to the email preferences defined in **Tools > Options > NAC > Email**.

Create a policy that detects vulnerabilities across your entire network. CounterACT uses published Macintosh updates to determine vulnerabilities.

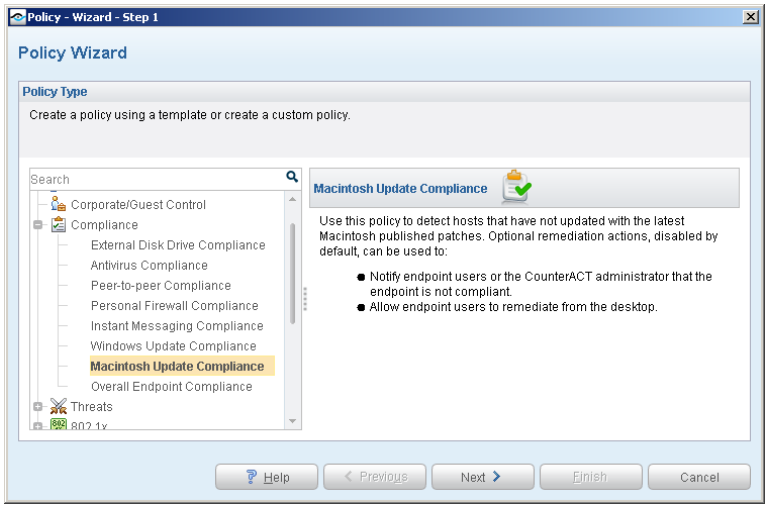
Endpoints must be managed by CounterACT, either by SecureConnector or remotely. There is an optional action, disabled by default, to install SecureConnector on unmanageable Macintosh endpoints.

Create a Policy for Macintosh Vulnerabilities

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



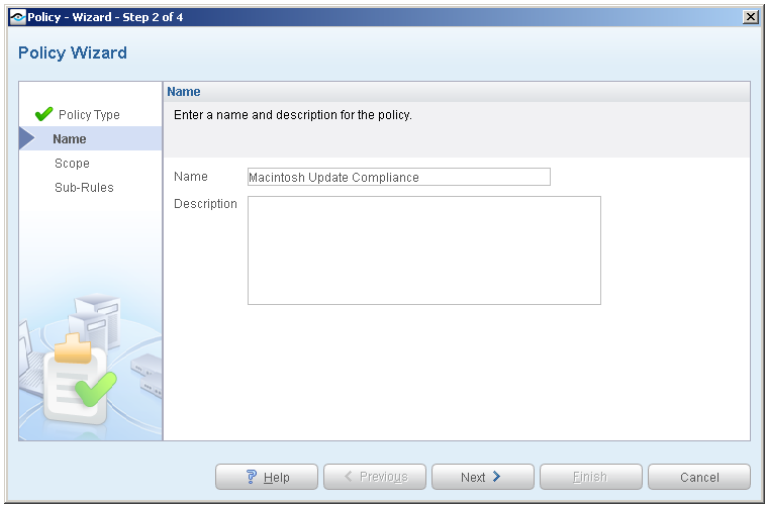
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Macintosh Update Compliance**.



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

2 Name the Policy

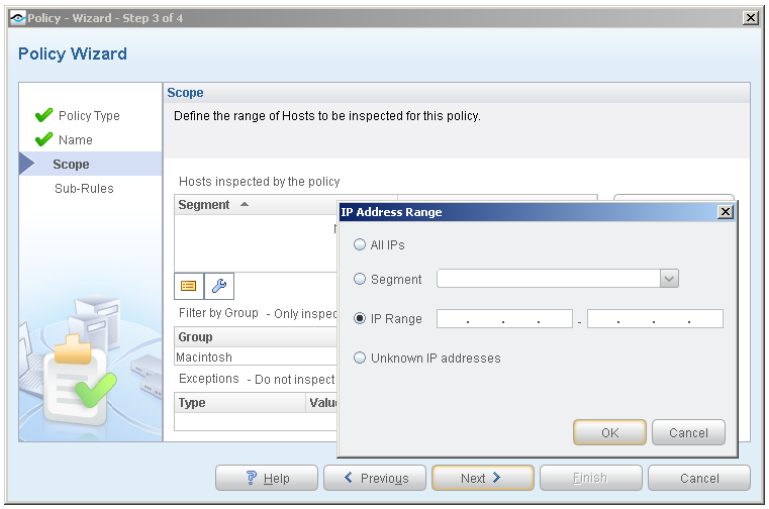
1. In the Name pane, a default policy name appears in the **Name** field.



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 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.

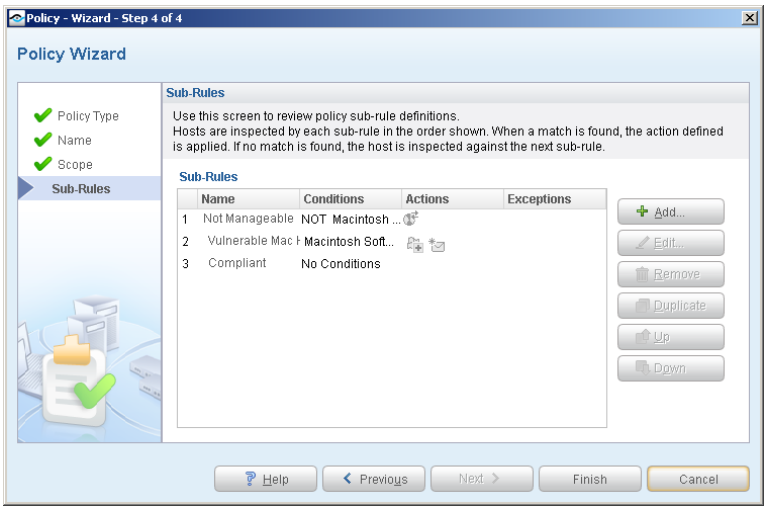
– **Unknown IP addresses** applies the policy to hosts whose IP addresses are not known. Not applicable for this policy template.

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

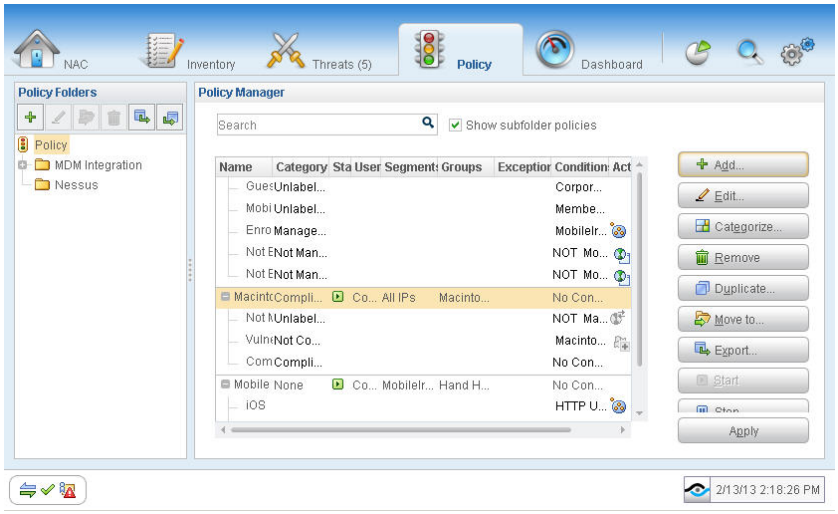
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). The *Add to Group* action is enabled by default for hosts that are found to be vulnerable.



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**.
4. A series of confirmation and completion dialog boxes opens. Select **Yes** or **OK** accordingly. On completion the policy is activated.

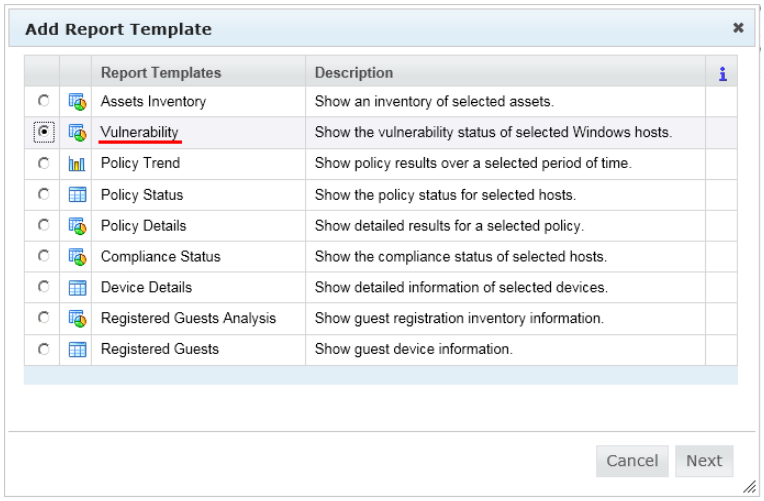
Generate Reports

After the policy runs, you can generate reports about vulnerable hosts, missing updates and their levels of severity. You can generate and view the reports immediately, or generate schedules to ensure that changes 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.

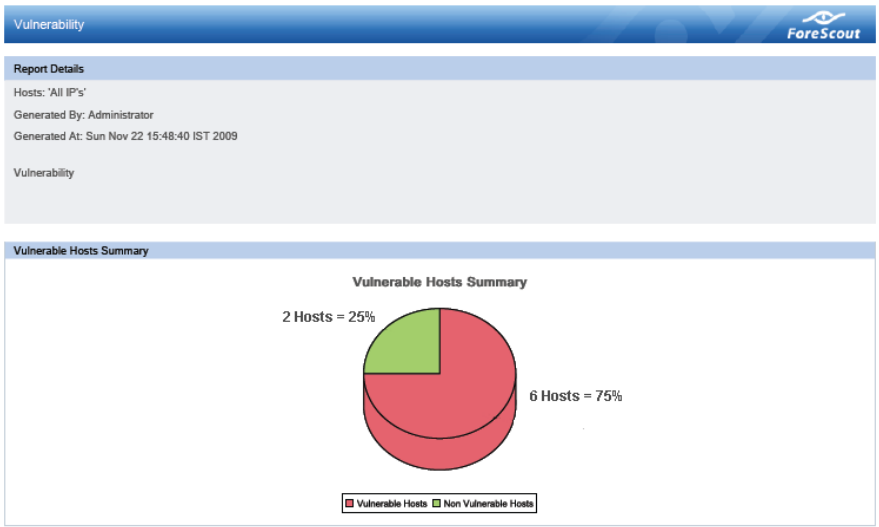
To generate a report:

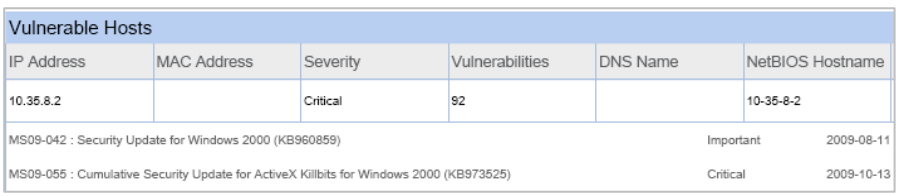
1. Select **Web Reports** from the Console **Reports** menu. The Reports portal opens.
2. Select **Add**. The Add Report Template dialog box opens.



3. Select the **Vulnerability** report template, and select **Next**. A report configuration window 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 Vulnerable Hosts Summary report was selected. This report gives you a pie chart breakdown of host vulnerability.





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