ForeScout CounterACT®

Control Network Vulnerabilities

How-to Guide

Version 8.0

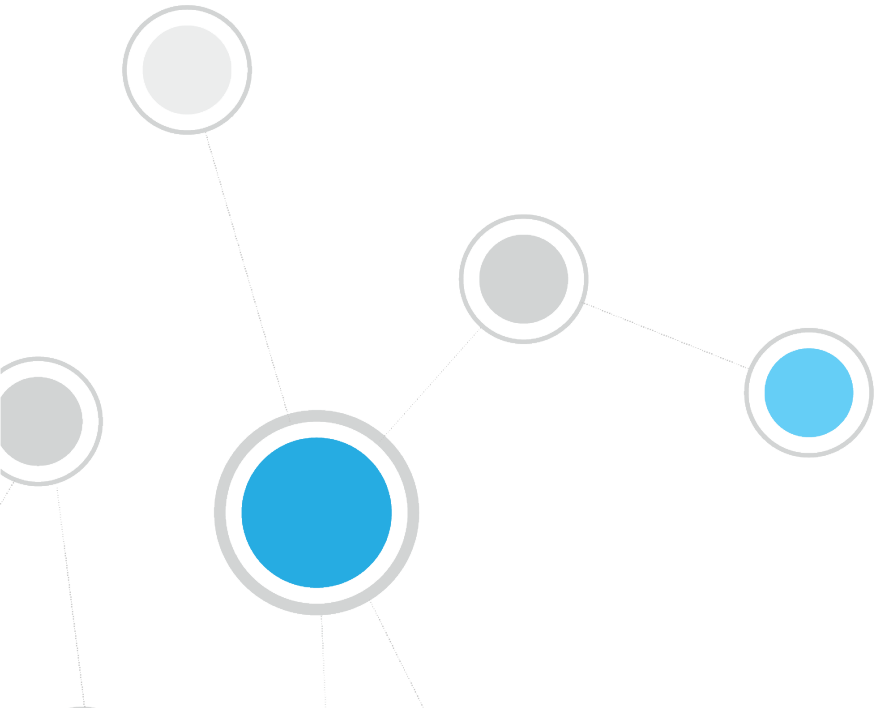


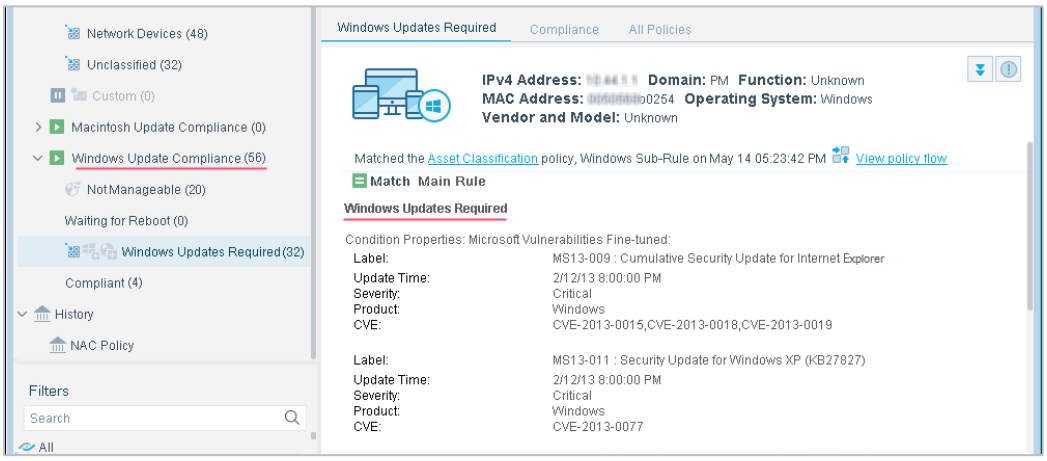
Table of Contents

About Controlling Network Vulnerabilities

ForeScout 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 CounterACT Administration Guide.

Prerequisites

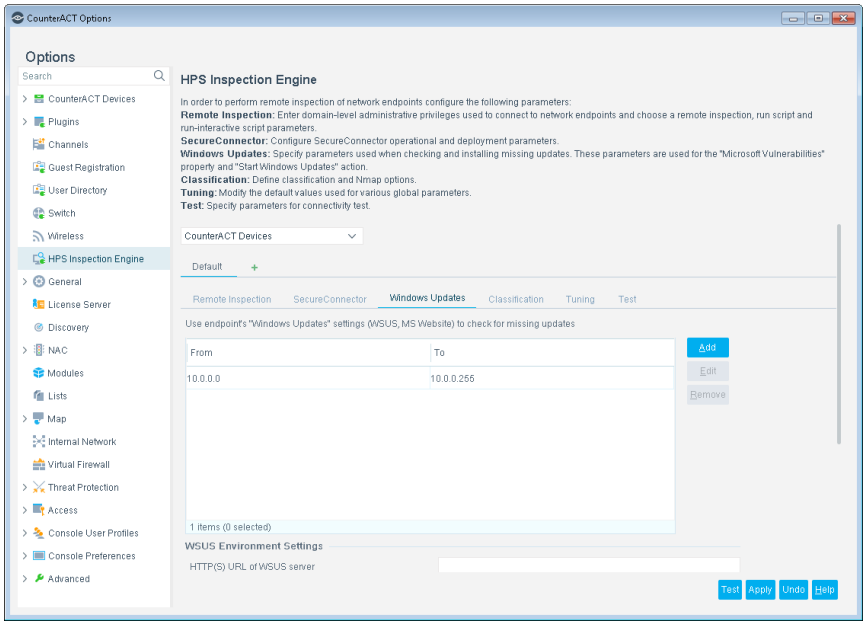
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the CounterACT Administration Guide for details.
- Verify that Windows and Macintosh groups appear in the Console, Home view, Filters pane. If not, run the Asset Classification template policy to create these groups.
- 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 CounterACT Administration Guide 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.

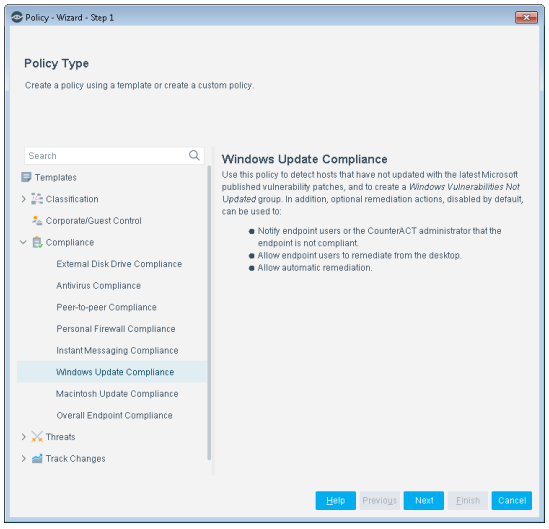
Remediation is performed from the Microsoft web site.

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

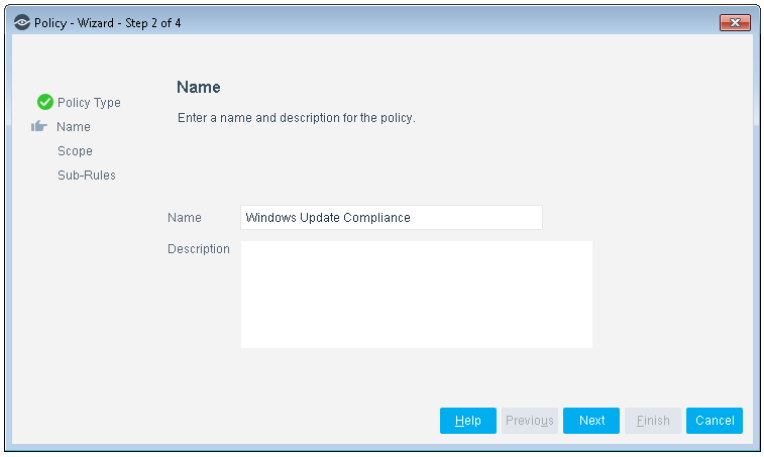
1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Windows Update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



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

Name the Policy

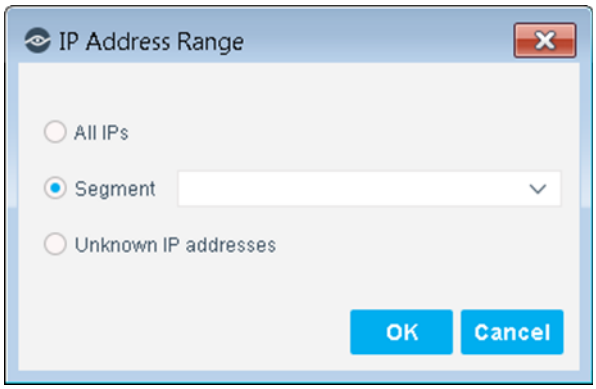
1. In the Name pane, a default policy name appears in the **Name** field.



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.

3 Choose Hosts to Inspect

1. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

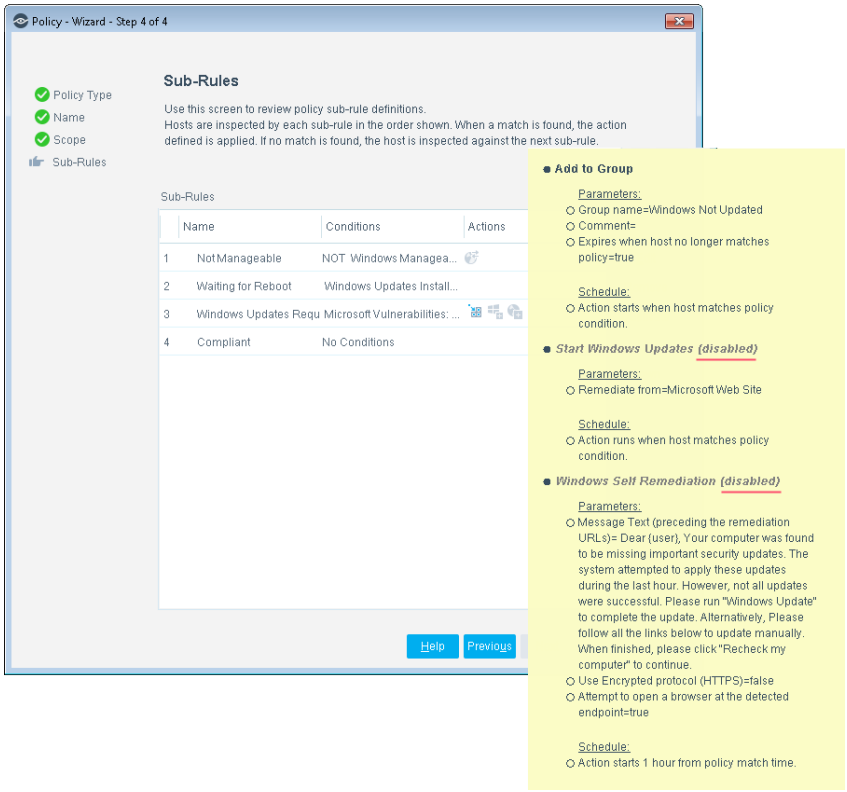
  Not applicable for this policy template.

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

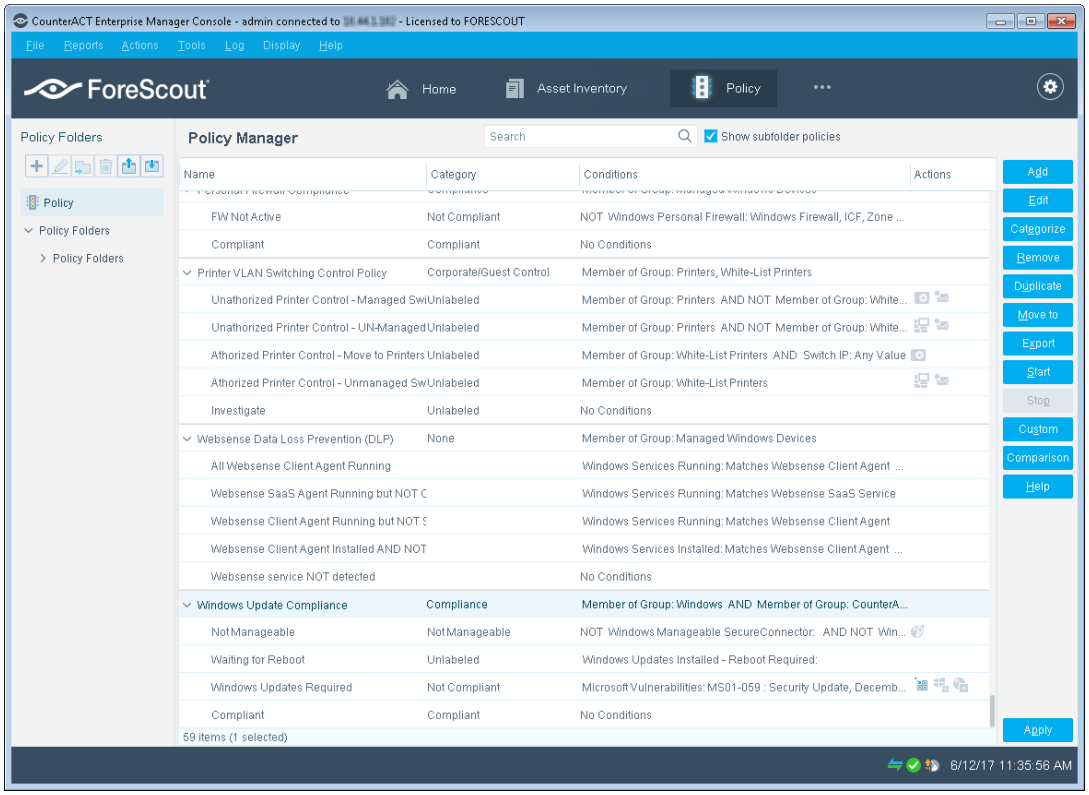
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). The Add to Group action is enabled by default. Optional remediation actions, disabled by default, can be used to start SecureConnector, start Windows Updates, 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.

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:

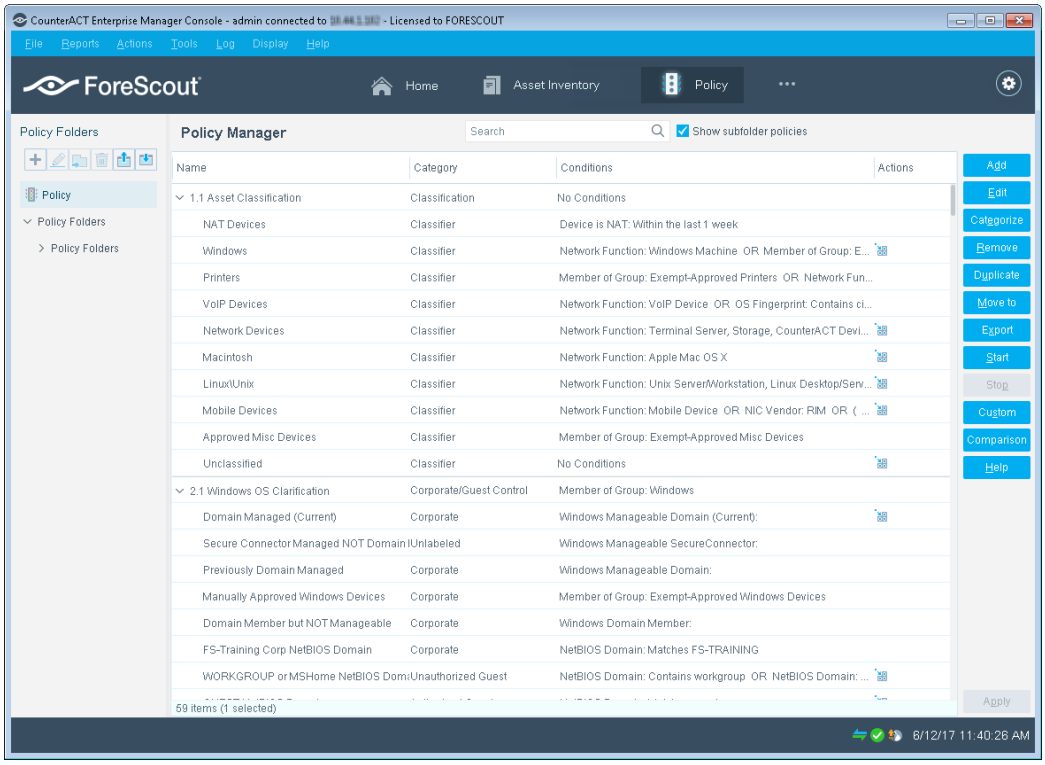
- Set up CounterACT to automatically provide the endpoints with appropriate patches for the missing Macintosh updates.
- Send an email message to a predefined user. The messages are sent according to the email preferences defined in **Tools > Options > NAC > Email**.

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

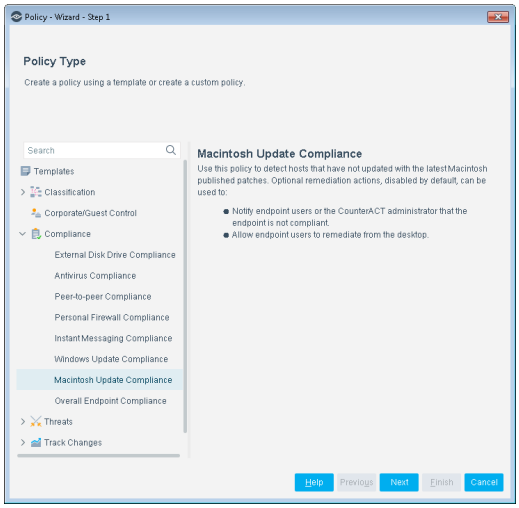
Endpoints must be managed by CounterACT, either by SecureConnector or remotely. There is an optional action, disabled by default, to install SecureConnector on unmanageable Macintosh endpoints.

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.



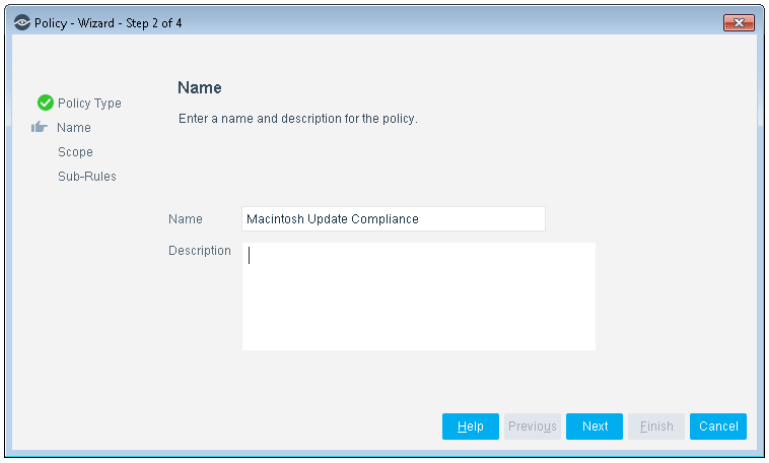
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Macintosh Update Compliance**.



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

Name the Policy

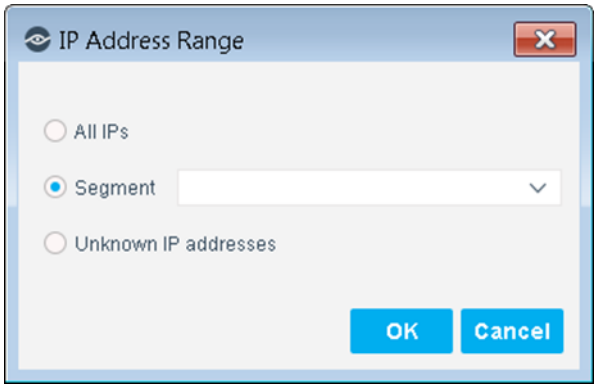
1. In the Name pane, a default policy name appears in the **Name** field.



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 which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

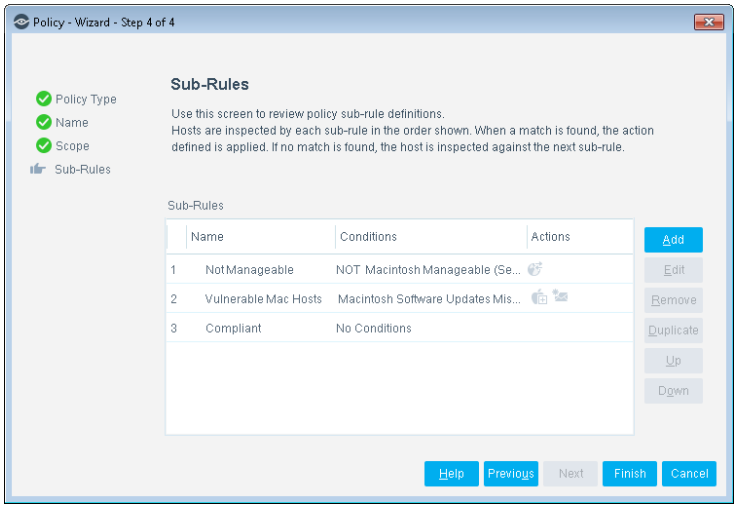
Not applicable for this policy template.

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

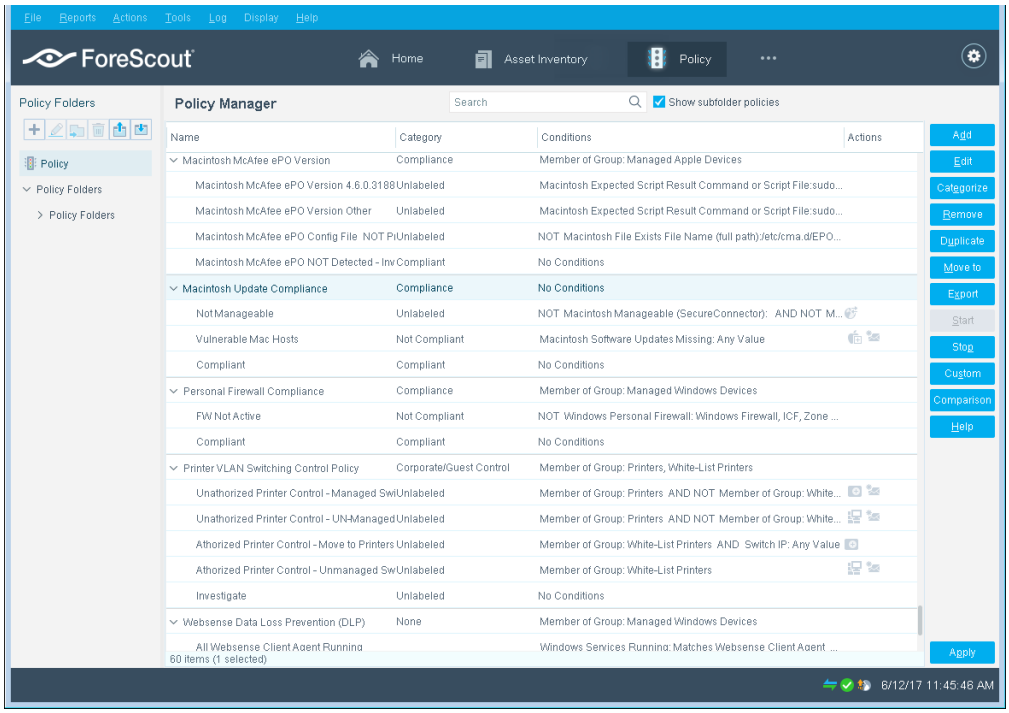
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). The Add to Group action is enabled by default for hosts that are found to be vulnerable.



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.

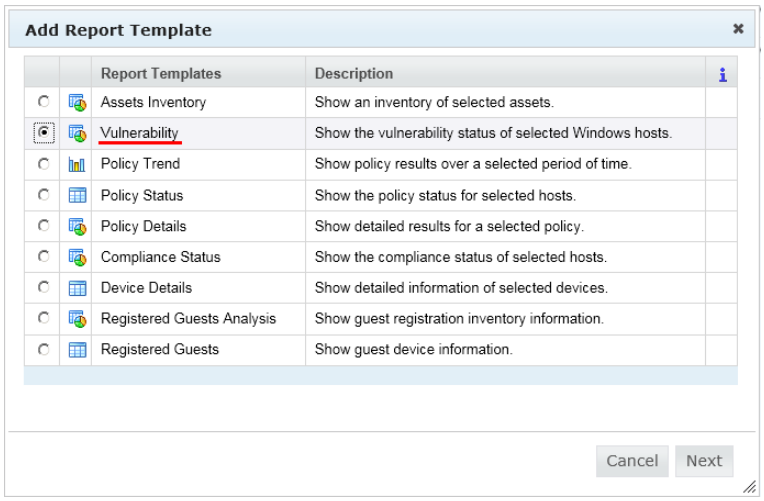
Generate Reports

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 schedule report generation.

The Reports Portal provides tools to customize reports and schedule automatic report generation. For more information about this portal, see the CounterACT Administration Guide.

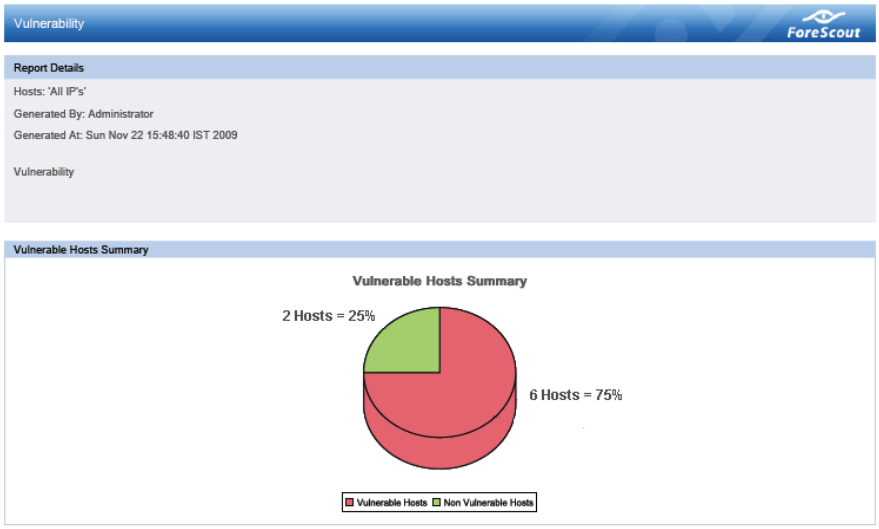
To generate a report:

1. Select **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.



Vulnerable Hosts

IP Address	MAC Address	Severity	Vulnerabilities	DNS Name	NetBIOS Hostname
10.35.8.2		Critical	92		10-35-8-2

MS09-042 : Security Update for Windows 2000 (KB960859)	Important	2009-08-11
MS09-055 : Cumulative Security Update for ActiveX Killbits for Windows 2000 (KB973525)	Critical	2009-10-13

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.

2. Select the plugin and then select **Help**.

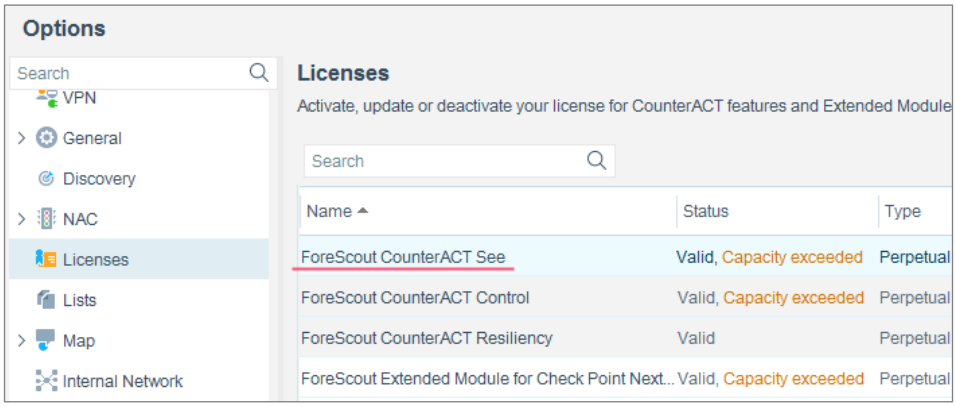
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-15 14:04