Forescout

Control Network Vulnerabilities

How-to Guide

Forescout version 8.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-03-20 14:13

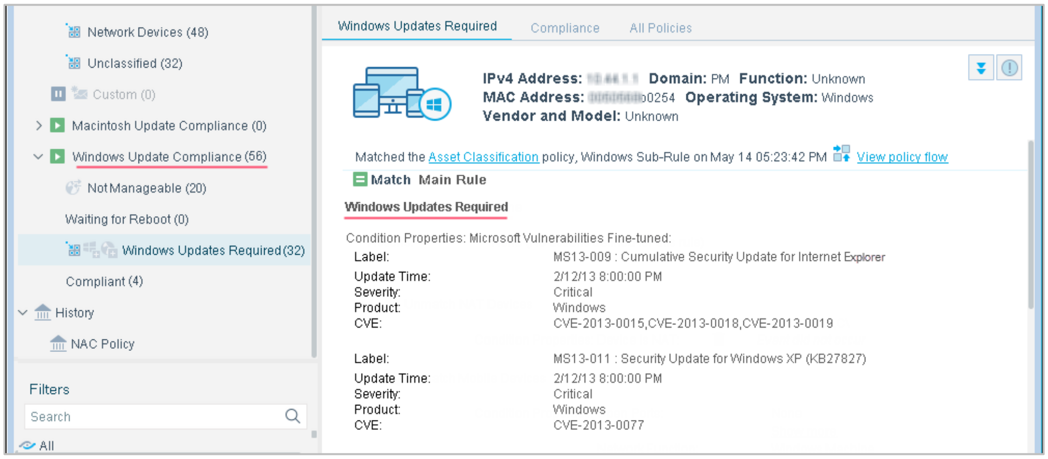
Table of Contents

About Controlling Network Vulnerabilities

Forescout® 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 Forescout 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.



IPv4 Address: [redacted] **Domain:** PM **Function:** Unknown
MAC Address: [redacted]0254 **Operating System:** Windows
Vendor and Model: Unknown

Matched the Asset Classification policy, Windows Sub-Rule on May 14 05:23:42 PM View policy flow

Match Main Rule

Windows Updates Required

Condition Properties: Microsoft Vulnerabilities Fine-tuned:

Label:	MS13-009 : Cumulative Security Update for Internet Explorer
Update Time:	2/12/13 8:00:00 PM
Severity:	Critical
Product:	Windows
CVE:	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019
Label:	MS13-011 : Security Update for Windows XP (KB27827)
Update Time:	2/12/13 8:00:00 PM
Severity:	Critical
Product:	Windows
CVE:	CVE-2013-0077

This How-to guide provides basic configuration instructions designed for a quick setup. For more information on the extended configuration options, refer to the Forescout Administration Guide.

Prerequisites

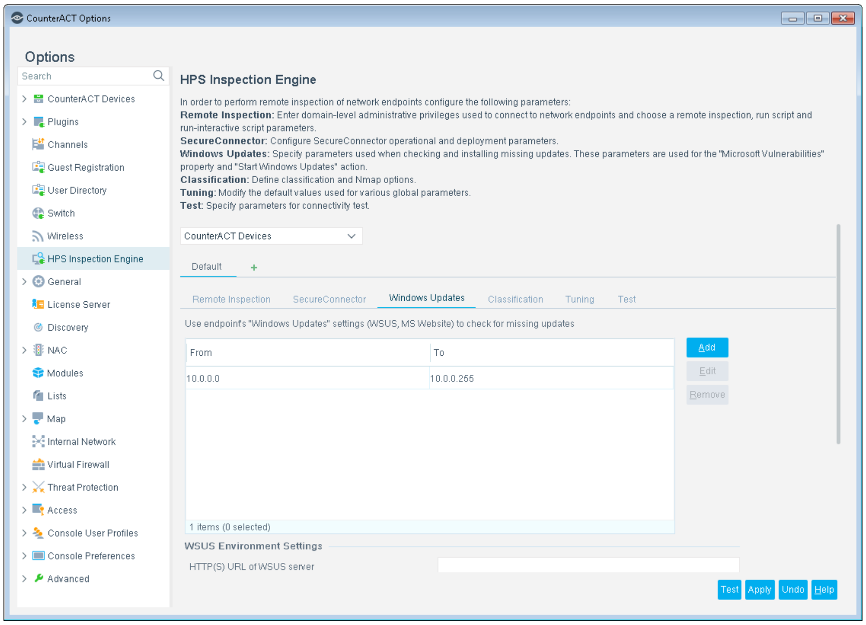
- Verify that your ForeScout system was set up using the Initial Setup Wizard. Refer to the *Forescout Administration Guide* for details.
- Verify that Windows and Macintosh groups appear in the Console, Home view, Filters pane. If not, run the Primary Classification template policy to create these groups.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

Creating a Policy for Microsoft Vulnerabilities

Use Forescout 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***: The Forescout platform 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.



HPS Inspection Engine

In order to perform remote inspection of network endpoints configure the following parameters:
Remote Inspection: Enter domain-level administrative privileges used to connect to network endpoints and choose a remote inspection, run script and run-interactive script parameters.
SecureConnector: Configure SecureConnector operational and deployment parameters.
Windows Updates: Specify parameters used when checking and installing missing updates. These parameters are used for the "Microsoft Vulnerabilities" property and "Start Windows Updates" action.
Classification: Define classification and Nmap options.
Tuning: Modify the default values used for various global parameters.
Test: Specify parameters for connectivity test.

Use endpoint's "Windows Updates" settings (WSUS, MS Website) to check for missing updates

From	To
10.0.0.0	10.0.0.255

1 items (0 selected)

WSUS Environment Settings

HTTP(S) URL of WSUS server

- ***Self-remediation***: The Forescout platform 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 Forescout *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 the Forescout platform, 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.

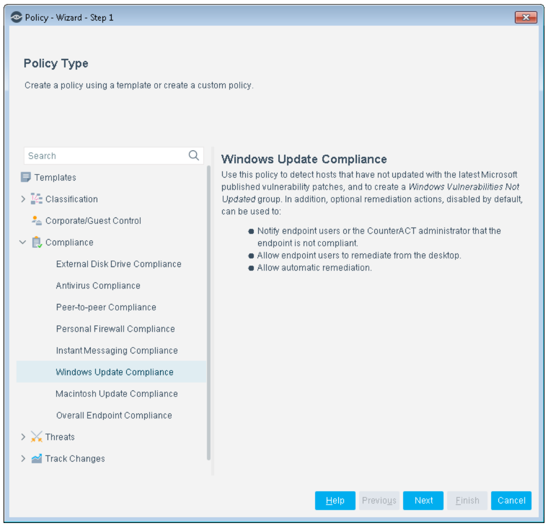
Follow these steps to create a Forescout policy for Microsoft Vulnerabilities:

- Create a Policy
- Name the Policy
- Choose Hosts to Inspect
- Finish Policy Creation
- Activate the policy

Create a Policy

To create a policy for Microsoft vulnerabilities:

1. Log in to the ForeScout 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 creaton.
4. Under **Templates**, expand the **Compliance** folder and select **Windows Update Compliance**.



Policy - Wizard - Step 1

Policy Type

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

Windows Update Compliance

Use this policy to detect hosts that have not updated with the latest Microsoft published vulnerability patches, and to create a *Windows Vulnerabilities Not Updated* group. In addition, optional remediation actions, disabled by default, can be used to:

- Notify endpoint users or the CounterACT administrator that the endpoint is not compliant.
- Allow endpoint users to remediate from the desktop.
- Allow automatic remediation.

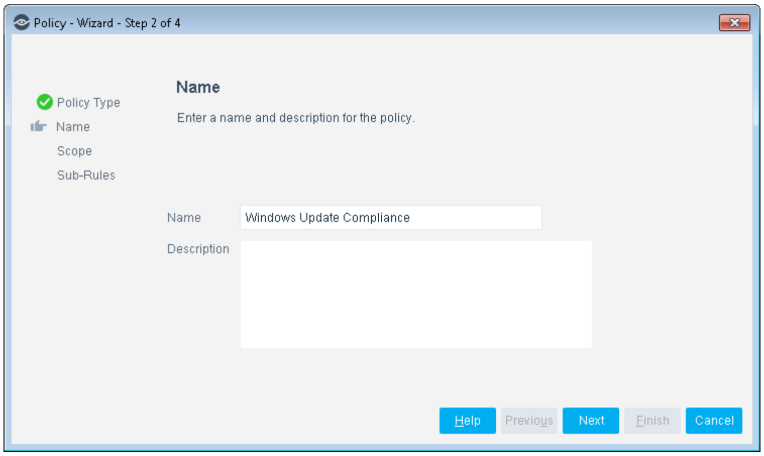
Search
Templates
Classification
Corporate/Guest Control
Compliance
External Disk Drive Compliance
Antivirus Compliance
Peer-to-peer Compliance
Personal Firewall Compliance
Instant Messaging Compliance
Windows Update Compliance
Macintosh Update Compliance
Overall Endpoint Compliance
Threats
Track Changes
Help
Previous
Next
Finish
Cancel

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

Name the Policy

To name the policy:

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



Policy - Wizard - Step 2 of 4

Name

Enter a name and description for the policy.

Name: Windows Update Compliance

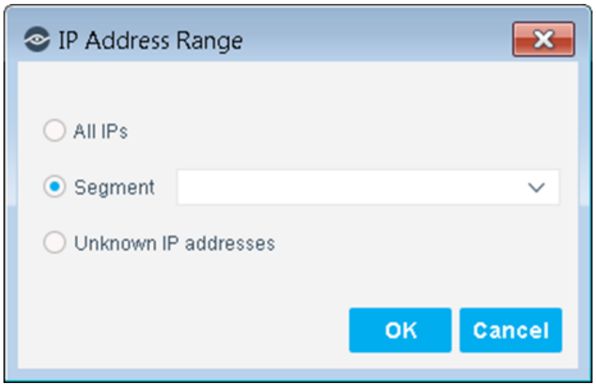
Description:

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

To choose hosts to inspect:

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



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

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 pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

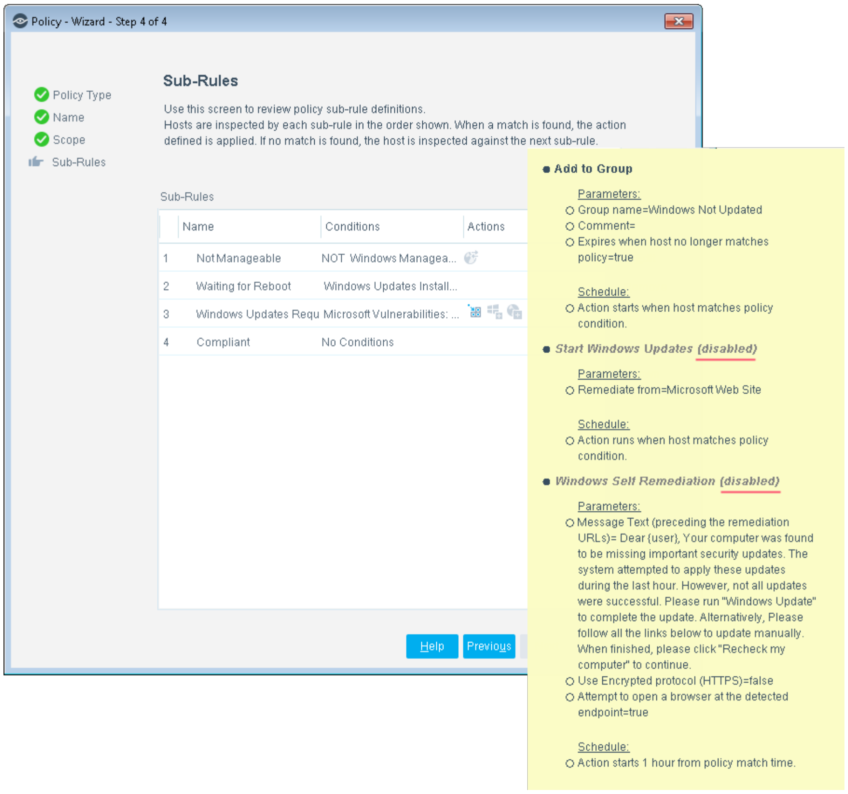
Not applicable for this policy template.

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 the Forescout platform 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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions
1	Not Manageable	NOT Windows Managea...	
2	Waiting for Reboot	Windows Updates Install...	
3	Windows Updates Requ	Microsoft Vulnerabilities: ...	
4	Compliant	No Conditions	

- **Add to Group**

  Parameters:
  - ○ Group name=Windows Not Updated
  - ○ Comment=
  - ○ Expires when host no longer matches policy=true

  Schedule:
  - ○ Action starts when host matches policy condition.

- ***Start Windows Updates (disabled)***

  Parameters:
  - ○ Remediate from=Microsoft Web Site

  Schedule:
  - ○ Action runs when host matches policy condition.

- ***Windows Self Remediation (disabled)***

  Parameters:
  - ○ Message Text (preceding the remediation URLs)= Dear {user}, Your computer was found to be missing important security updates. The system attempted to apply these updates during the last hour. However, not all updates were successful. Please run "Windows Update" to complete the update. Alternatively, Please follow all the links below to update manually. When finished, please click "Recheck my computer" to continue.
  - ○ Use Encrypted protocol (HTTPS)=false
  - ○ Attempt to open a browser at the detected endpoint=true

  Schedule:
  - ○ Action starts 1 hour from policy match time.

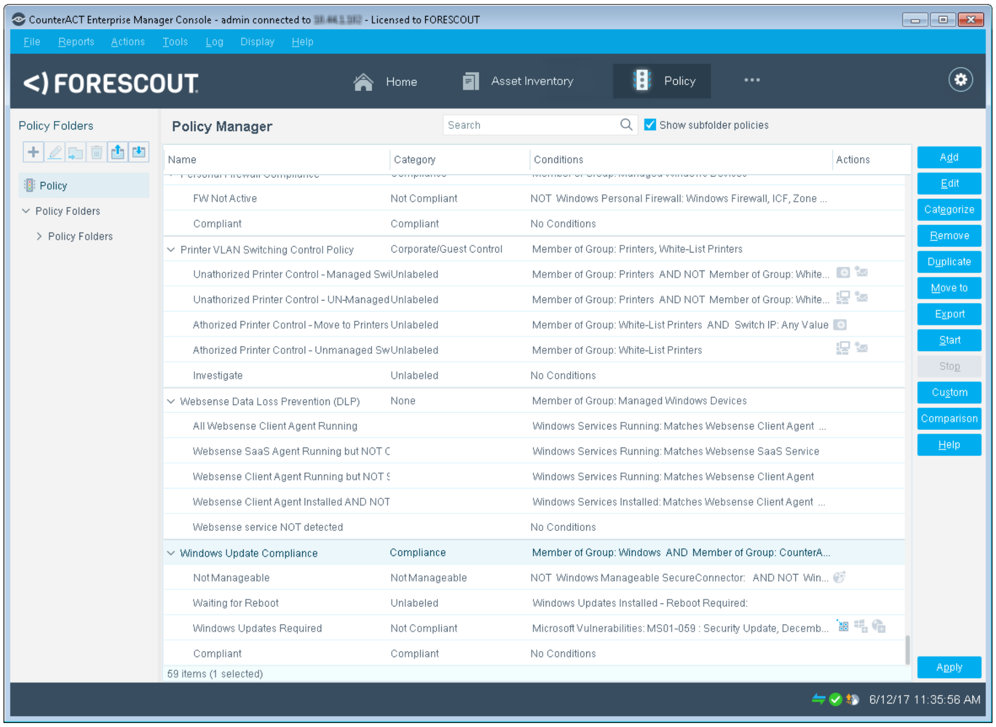
To finish creating the policy:

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

Activate the policy

To activate the policy:

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



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to FORESCOUT

Name	Category	Conditions	Actions
Personal Firewall Compliance	Compliance	Member of Group: Managed Windows Devices	
FW Not Active	Not Compliant	NOT Windows Personal Firewall: Windows Firewall, ICF, Zone ...	
Compliant	Compliant	No Conditions	
Printer VLAN Switching Control Policy	Corporate/Guest Control	Member of Group: Printers, White-List Printers	
Unathorized Printer Control - Managed Swi	Unlabeled	Member of Group: Printers AND NOT Member of Group: White...	
Unathorized Printer Control - UN-Managed	Unlabeled	Member of Group: Printers AND NOT Member of Group: White...	
Athorized Printer Control - Move to Printers	Unlabeled	Member of Group: White-List Printers AND Switch IP: Any Value	
Athorized Printer Control - Unmanaged Sw	Unlabeled	Member of Group: White-List Printers	
Investigate	Unlabeled	No Conditions	
Websense Data Loss Prevention (DLP)	None	Member of Group: Managed Windows Devices	
All Websense Client Agent Running		Windows Services Running: Matches Websense Client Agent ...	
Websense SaaS Agent Running but NOT C		Windows Services Running: Matches Websense SaaS Service	
Websense Client Agent Running but NOT S		Windows Services Running: Matches Websense Client Agent	
Websense Client Agent Installed AND NOT		Windows Services Installed: Matches Websense Client Agent ...	
Websense service NOT detected		No Conditions	
Windows Update Compliance	Compliance	Member of Group: Windows AND Member of Group: CounterA...	
Not Manageable	Not Manageable	NOT Windows Manageable SecureConnector: AND NOT Win...	
Waiting for Reboot	Unlabeled	Windows Updates Installed - Reboot Required:	
Windows Updates Required	Not Compliant	Microsoft Vulnerabilities: MS01-059 : Security Update, Decemb...	
Compliant	Compliant	No Conditions	

59 items (1 selected)

6/12/17 11:35:56 AM

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 Forescout 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 Forescout 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. The Forescout platform uses published Macintosh updates to determine vulnerabilities.

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

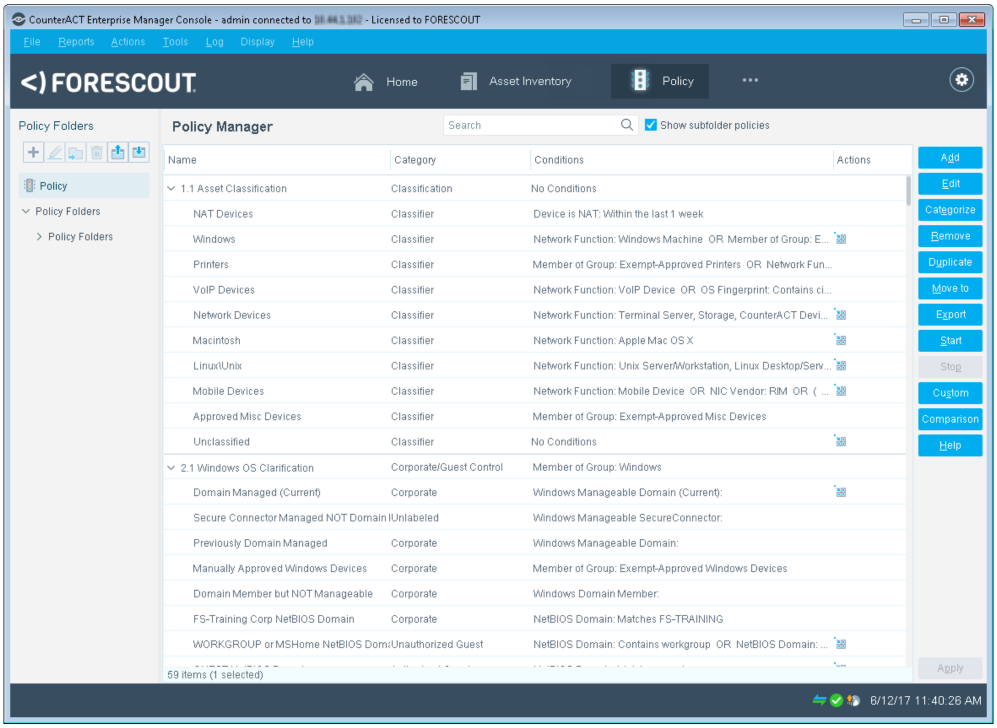
Follow these steps to create a Forescout policy for Macintosh Vulnerabilities:

- Create a Policy
- Name the Policy
- Choose Hosts to Inspect
- Finish Policy Creation
- Finish Policy Creation

Create a Policy

To create a policy for Macintosh vulnerabilities:

1. Log in to the ForeScout Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to FORESCOUT

☑ Show subfolder policies

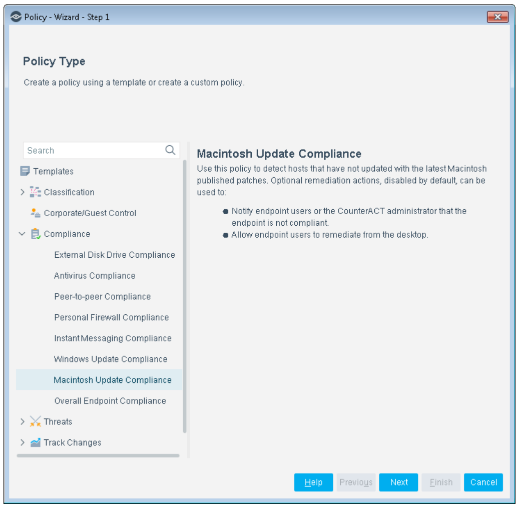
Name	Category	Conditions	Actions
1.1 Asset Classification	Classification	No Conditions	
NAT Devices	Classifier	Device is NAT: Within the last 1 week	
Windows	Classifier	Network Function: Windows Machine OR Member of Group: E...	
Printers	Classifier	Member of Group: Exempt-Approved Printers OR Network Fun...	
VoIP Devices	Classifier	Network Function: VoIP Device OR OS Fingerprint: Contains ci...	
Network Devices	Classifier	Network Function: Terminal Server, Storage, CounterACT Devi...	
Macintosh	Classifier	Network Function: Apple Mac OS X	
Linux\Unix	Classifier	Network Function: Unix Server/Workstation, Linux Desktop/Serv...	
Mobile Devices	Classifier	Network Function: Mobile Device OR NIC Vendor: RIM OR (...	
Approved Misc Devices	Classifier	Member of Group: Exempt-Approved Misc Devices	
Unclassified	Classifier	No Conditions	
2.1 Windows OS Clarification	Corporate/Guest Control	Member of Group: Windows	
Domain Managed (Current)	Corporate	Windows Manageable Domain (Current):	
Secure Connector Managed NOT Domain I	Unlabeled	Windows Manageable SecureConnector:	
Previously Domain Managed	Corporate	Windows Manageable Domain:	
Manually Approved Windows Devices	Corporate	Member of Group: Exempt-Approved Windows Devices	
Domain Member but NOT Manageable	Corporate	Windows Domain Member:	
FS-Training Corp NetBIOS Domain	Corporate	NetBIOS Domain: Matches FS-TRAINING	
WORKGROUP or MSHome NetBIOS Dom:	Unauthorized Guest	NetBIOS Domain: Contains workgroup OR NetBIOS Domain: ...	

59 items (1 selected)

6/12/17 11:40:26 AM

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**.



Policy Type

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

Macintosh Update Compliance

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

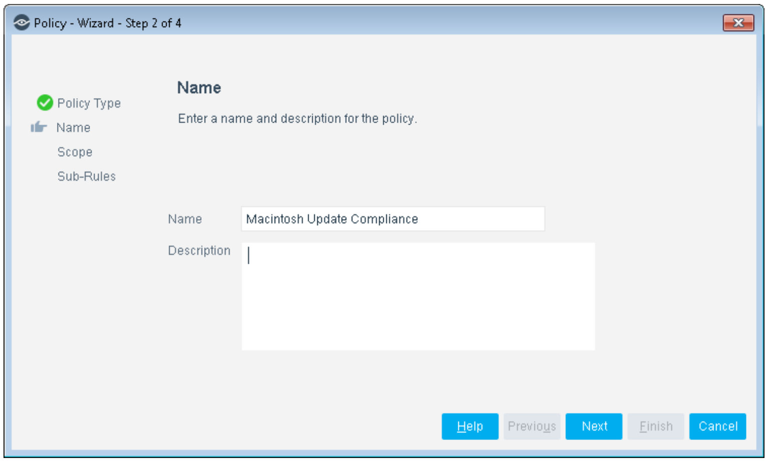
- Notify endpoint users or the CounterACT administrator that the endpoint is not compliant.
- Allow endpoint users to remediate from the desktop.

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

Name the Policy

To name the policy:

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



Name

Enter a name and description for the policy.

Name: Macintosh Update Compliance

Description:

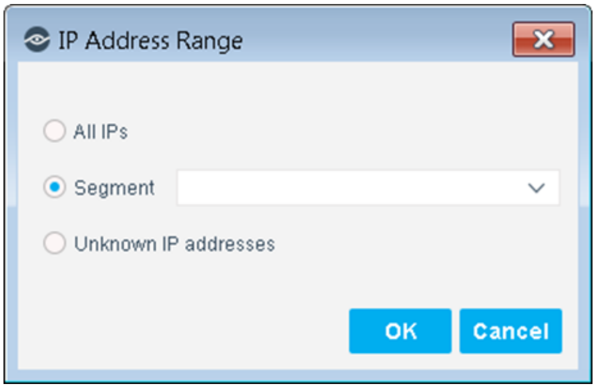
2. Accept the default name or create a new name, and add a description.

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

Choose Hosts to Inspect

To choose hosts to inspect:

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



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

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 pane.

– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

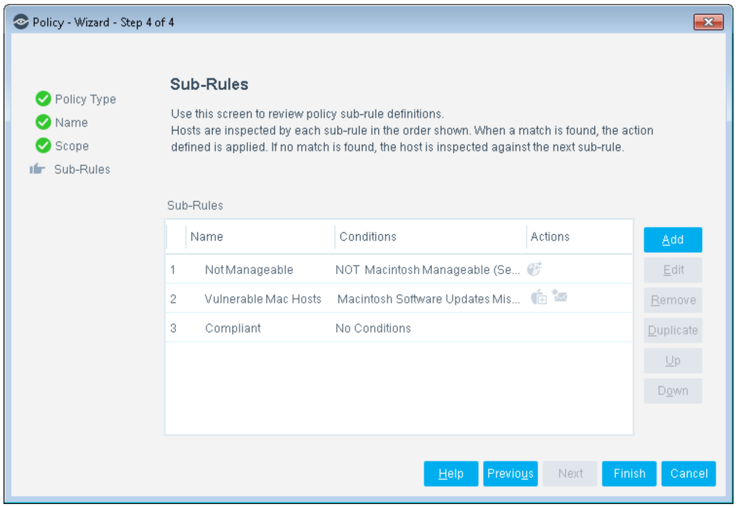
Not applicable for this policy template.

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 the Forescout platform 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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions
1	Not Manageable	NOT Macintosh Manageable (Se...	
2	Vulnerable Mac Hosts	Macintosh Software Updates Mis...	
3	Compliant	No Conditions	

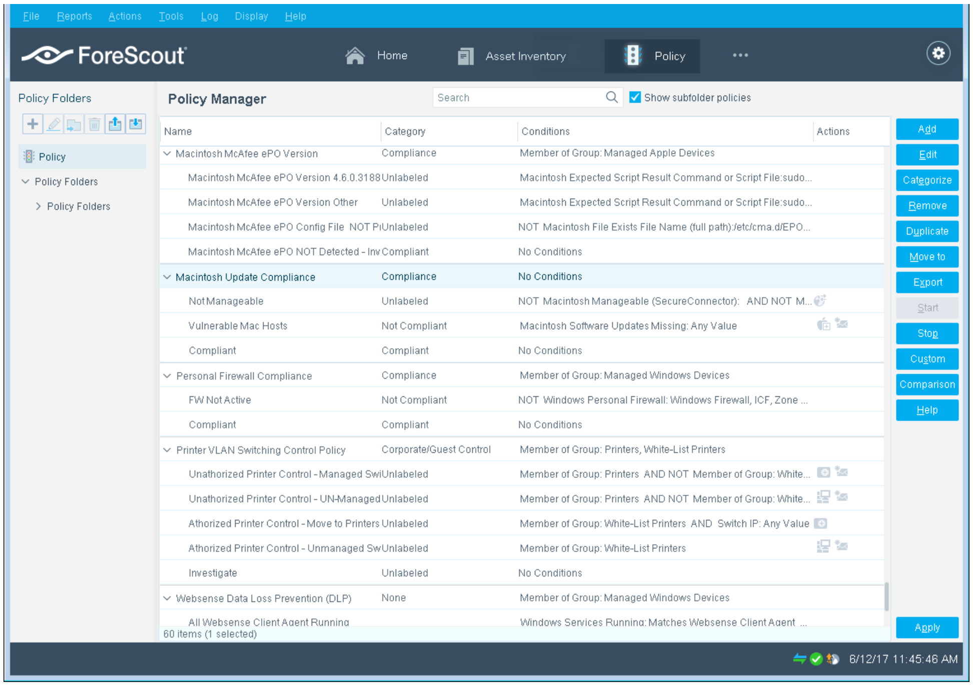
To finish creating the policy:

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

Activate the Policy

To activate the policy:

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



Name	Category	Conditions	Actions
Macintosh McAfee ePO Version	Compliance	Member of Group: Managed Apple Devices	
Macintosh McAfee ePO Version 4.6.0.3188	Unlabeled	Macintosh Expected Script Result Command or Script File:sudo...	
Macintosh McAfee ePO Version Other	Unlabeled	Macintosh Expected Script Result Command or Script File:sudo...	
Macintosh McAfee ePO Config File NOT Pı	Unlabeled	NOT Macintosh File Exists File Name (full path):/etc/cma.d/EPO...	
Macintosh McAfee ePO NOT Detected - Inv	Compliant	No Conditions	
Macintosh Update Compliance	Compliance	No Conditions	
Not Manageable	Unlabeled	NOT Macintosh Manageable (SecureConnector): AND NOT M...	
Vulnerable Mac Hosts	Not Compliant	Macintosh Software Updates Missing: Any Value	
Compliant	Compliant	No Conditions	
Personal Firewall Compliance	Compliance	Member of Group: Managed Windows Devices	
FW Not Active	Not Compliant	NOT Windows Personal Firewall: Windows Firewall, ICF, Zone ...	
Compliant	Compliant	No Conditions	
Printer VLAN Switching Control Policy	Corporate/Guest Control	Member of Group: Printers, White-List Printers	
Unathorized Printer Control - Managed Swi	Unlabeled	Member of Group: Printers AND NOT Member of Group: White...	
Unathorized Printer Control - UN-Managed	Unlabeled	Member of Group: Printers AND NOT Member of Group: White...	
Athorized Printer Control - Move to Printers	Unlabeled	Member of Group: White-List Printers AND Switch IP: Any Value	
Athorized Printer Control - Unmanaged Sw	Unlabeled	Member of Group: White-List Printers	
Investigate	Unlabeled	No Conditions	
Websense Data Loss Prevention (DLP)	None	Member of Group: Managed Windows Devices	
All Websense Client Agent Running		Windows Services Running: Matches Websense Client Agent ...	

60 items (1 selected)

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

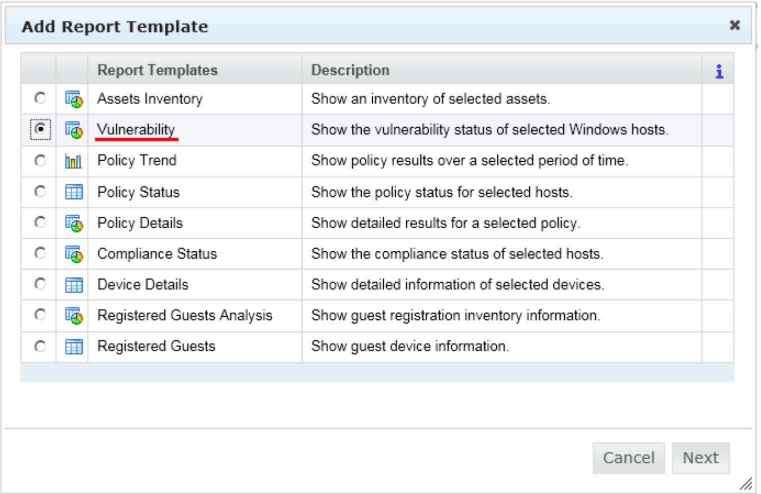
Generating Reports

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 Forescout 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.

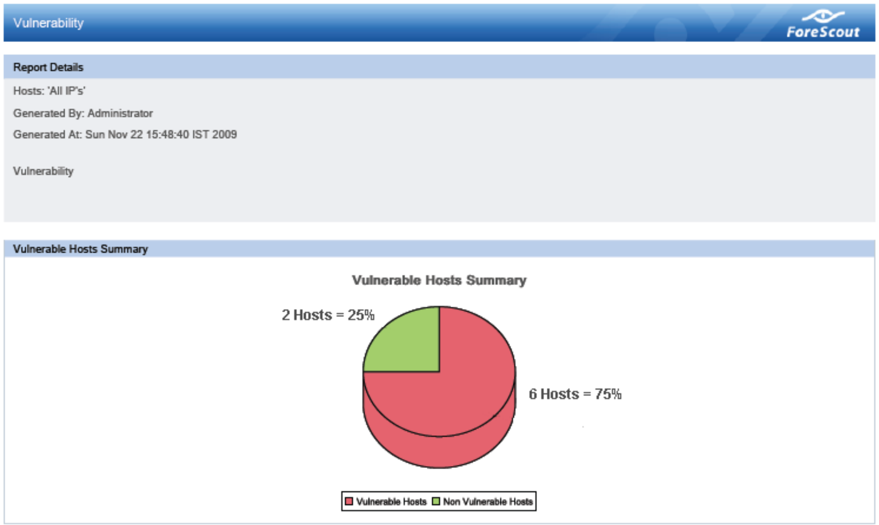


		Report Templates	Description
○		Assets Inventory	Show an inventory of selected assets.
●		Vulnerability	Show the vulnerability status of selected Windows hosts.
○		Policy Trend	Show policy results over a selected period of time.
○		Policy Status	Show the policy status for selected hosts.
○		Policy Details	Show detailed results for a selected policy.
○		Compliance Status	Show the compliance status of selected hosts.
○		Device Details	Show detailed information of selected devices.
○		Registered Guests Analysis	Show guest registration inventory information.
○		Registered Guests	Show guest device information.

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.



Vulnerability

Report Details

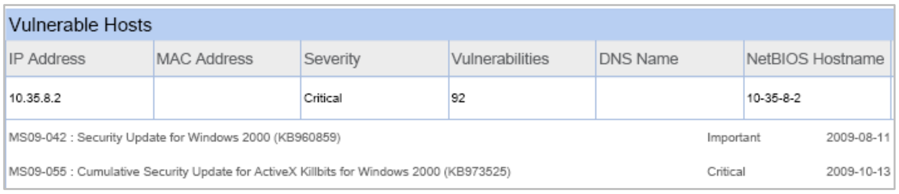
Hosts: 'All IP's'

Generated By: Administrator

Generated At: Sun Nov 22 15:48:40 IST 2009

Vulnerability

Vulnerable Hosts Summary



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 Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

🗎 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

🗎 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).