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

Legal Notice
© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Table of Contents

About Controlling Network Vulnerabilities ................................................... 4

Prerequisites ................................................................................................ 4

Creating a Policy for Microsoft Vulnerabilities ............................................. 5
  Create a Policy .......................................................................................... 6
  Name the Policy ...................................................................................... 7
  Choose Hosts to Inspect .......................................................................... 7
  Finish Policy Creation ............................................................................. 8
  Activate the policy .................................................................................. 8

Creating a Policy for Macintosh Vulnerabilities .......................................... 9
  Create a Policy ...................................................................................... 10
  Name the Policy .................................................................................... 10
  Choose Hosts to Inspect ........................................................................ 11
  Finish Policy Creation ............................................................................ 12
  Activate the Policy ................................................................................ 13

Generating Reports ..................................................................................... 14

Additional Forescout Documentation .......................................................... 15
  Documentation Downloads ..................................................................... 15
  Documentation Portal ............................................................................. 16
  Forescout Help Tools ............................................................................. 16
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.

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.

- **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 creation.
4. Under **Templates**, expand the **Compliance** folder and select **Windows Update Compliance**.
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.

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.

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.

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.
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**
Control Network Vulnerabilities
How-to Guide

- Choose Hosts to Inspect
- Finish Policy Creation
- Activate the Policy

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.
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

To 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**

**To 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 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.

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.
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.
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 Summary](image)

### 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 Technical Documentation Page](#), and 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 Support Portal](#)

> Software downloads are also available from these portals.
To identify your licensing mode:

- From the Console, select Help > About Forescout.

**Forescout Technical Documentation Page**

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

**To access the Technical Documentation Page:**

- Go to https://www.Forescout.com/company/technical-documentation/

**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 Support Portal**

The Downloads page on the Forescout Customer Support 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 Customer Support 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.

**To access the Documentation Portal:**

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

**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 Administration Guide from the Help menu.
### Plugin Help Files

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

### Documentation Portal

- Select **Documentation Portal** from the **Help** menu to access the [Documentation Portal](#).