Forescout

Ensure Antivirus Compliance

How-to Guide

Forescout versions 8.1 and 8.2
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 Ensuring Antivirus Compliance ........................................................... 4

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

Create and Apply an Antivirus Policy ............................................................ 5
  Select the Antivirus Compliance Template .................................................. 5
  Name the Policy ....................................................................................... 6
  Choose Hosts to Inspect ......................................................................... 7
  Choose Vendors to Manage / Define Period .............................................. 8
  Finish Policy Creation .............................................................................. 9
  Activate the Policy .................................................................................. 9

Evaluate Host Compliance ......................................................................... 11

Generate Reports ........................................................................................ 12

Additional Forescout Documentation .......................................................... 13
  Documentation Downloads ...................................................................... 13
  Documentation Portal ............................................................................. 14
  Forescout Help Tools ............................................................................. 14
About Ensuring Antivirus Compliance

Forescout® provides powerful tools that let you continuously track and control Antivirus installations to ensure that your hosts comply with your organization’s Antivirus policies.

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

• Use a wizard-based Forescout template to create an Antivirus Compliance policy. The policy detects hosts at which Antivirus applications are:
  – not installed
  – not running
  – not up-to-date

The policy places hosts in groups that reflect their status. You can view these groups at the Console.

• Review an extensive range of information about each device and about the users connected to them.

• Generate real-time and trend reports on Antivirus network compliance.

After running a policy to detect non complaint hosts, you can optionally enable automated remediation and self-remediation to handle non-compliant hosts.

ียว The policy described in this guide inspects only Windows machines. To inspect Macintosh machines, use this general procedure to create Macintosh Update Compliance policy.

묘 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 the Corporate Hosts and Windows groups appear in the Console, Filters pane. If not, run the Primary Classification and Corporate/Guest Control template policies to create these groups. Refer to the Forescout Administration Guide for details.
Create and Apply an Antivirus Policy

Follow these steps to detect the Antivirus application status on network endpoints using a policy template.

- Select the Antivirus Compliance Template
- Name the Policy
- Choose Hosts to Inspect
- Choose Vendors to Manage / Define Period
- Finish Policy Creation
- Activate the Policy

Select the Antivirus Compliance Template

To select the Antivirus Compliance template:

1. Log into 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 **Antivirus Compliance**.

![Antivirus Compliance Policy](image)

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 Pane](image)

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 dialog box]

   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 Antivirus pane opens.
Choose Vendors to Manage / Define Period

To choose vendors to manage / define period:

1. New vendors may be added to this list in between Forescout version releases. To automatically include newly supported vendors/versions in the inspection, select **Any vendor**.

2. To select specific vendors to detect, select **Specify vendors** and select the individual vendors.

   The value in the **Antivirus updated** field indicates how recently the last Antivirus signature update must have been performed on the host. If the update was performed previous to this, the host is not considered compliant.

   - The Antivirus application must be running to be detected.

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 automatically places non-compliant endpoints into the following groups:

- Antivirus Not Installed
- Antivirus Not Running
- Antivirus Not Updated

*Other actions for handling the non-compliant endpoints policy are disabled by default. Activate these actions only after you run the policy and review the generated groups.*

**To finish the 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 dialog boxes opens. Select **Yes** or **OK** accordingly. On completion, the policy is activated.

   The Forescout platform detects Antivirus applications that are either not installed, not running or have not been updated.

5. On the **Console** toolbar, select the **Home** view.

6. In the **Filters** pane, expand the **Groups** folder and scroll to view the detected AntiVirus groups.
Evaluate Host Compliance

After activating the policy, you can view an extensive range of details about antivirus host compliance.

To evaluate antivirus host compliance:

1. On the Console toolbar, select the Home view.
2. In the Views pane, expand the Policy folder and select your AntiVirus Compliance policy.
3. In the Detections pane, select an antivirus host. Host information is displayed in the Details pane.
4. In the Filters pane, expand the Groups folder and select the Antivirus Not Installed, Antivirus Not Running or Antivirus Not Updated group.
   The hosts detected without antivirus installed, running or updated are displayed in the Detections pane.
5. To customize the information displayed about antivirus hosts, 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 non-compliant hosts. 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 Web Reports from the Console Reports menu. The Reports portal opens.
3. Select the Policy Trend or Compliance Status 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 Trend report was selected. This report gives you a breakdown of compliance with your Antivirus policy over time.
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.