ForeScout

Ensure Antivirus Compliance

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Ensuring Antivirus Compliance

CounterACT provides powerful tools that let you continuously track and control Antivirus installations to ensure that your hosts are in compliance with your organization's Antivirus policies.

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

- Use a wizard-based CounterACT 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.

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

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

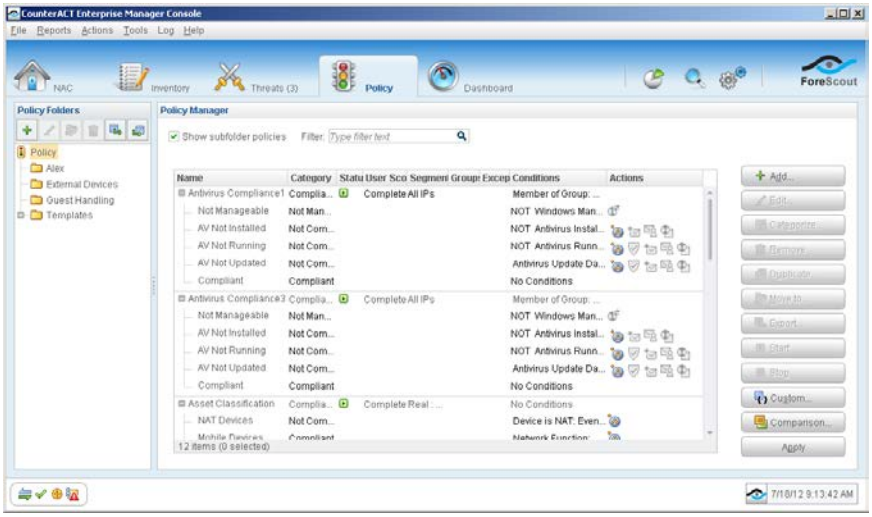
- Verify that your CounterACT system was set up using the Initial Setup Wizard. Refer to the Console Online Help for details.
- Verify that the *Corporate Hosts* and *Windows* groups appear in the Console, Filters pane. If not, run the *Asset Classification* and *Corporate/Guest Control* template policies to create these groups. Refer to the Console Online Help for details.

Create and Apply an Antivirus Policy

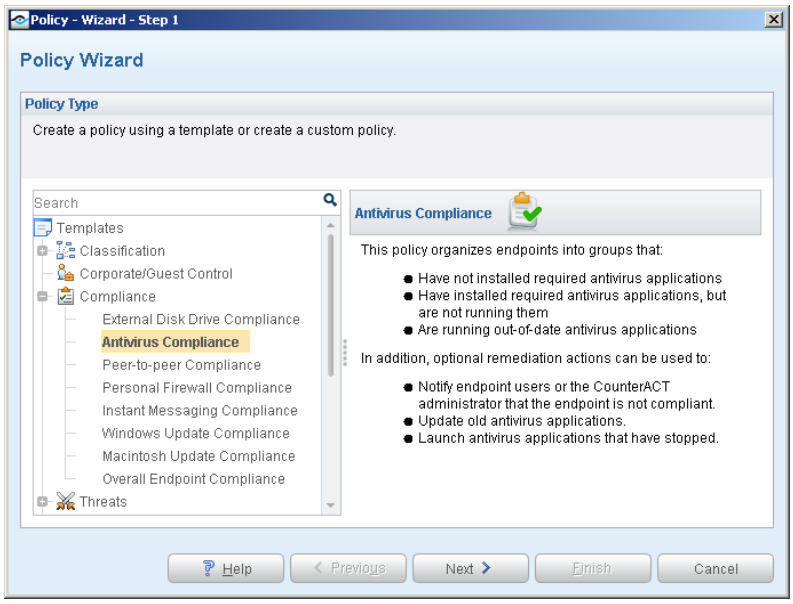
Follow these steps to detect the Antivirus application status on network endpoints using a policy template.

Select the Antivirus Compliance Template

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



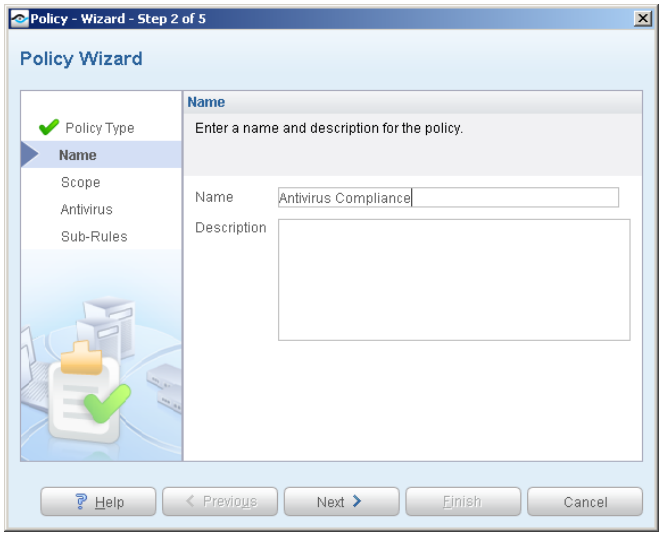
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Antivirus Compliance**.



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

2 Name the Policy

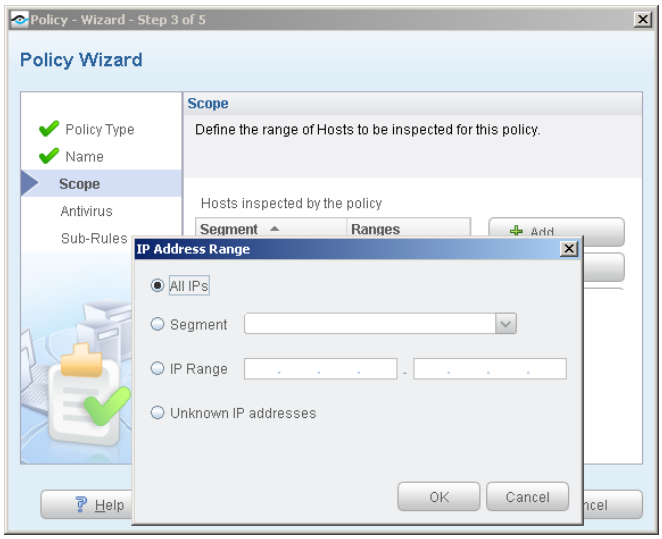
1. In the Name pane, a default policy name appears in the **Name** field.



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.

3 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 Antivirus pane opens.

4 Choose Vendors to Manage / Define Period

1. New vendors may be added to this list in between CounterACT 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.

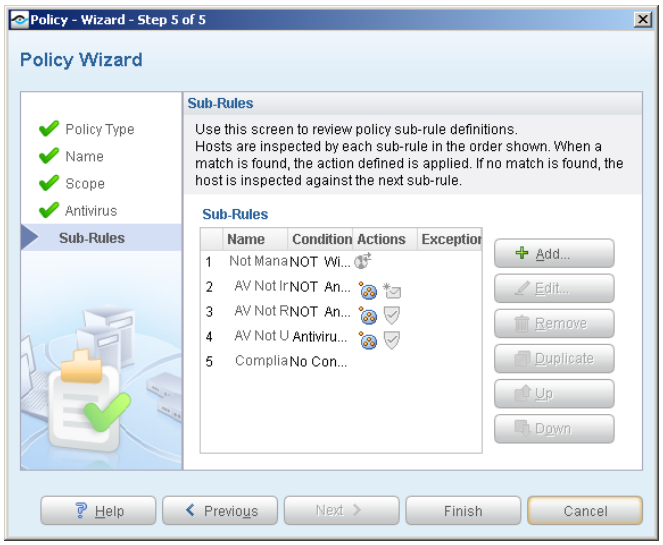
   The value in the **Antivirus updated** field indicates how recently the last Antivirus signature update must have been performed on the host. If the update was performed previous to this, the host is not considered compliant.

The Antivirus application must be running to be detected.

3. Select **Next**. The Sub-Rules pane opens.

5 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 automatically places non-compliant endpoints into the following groups:

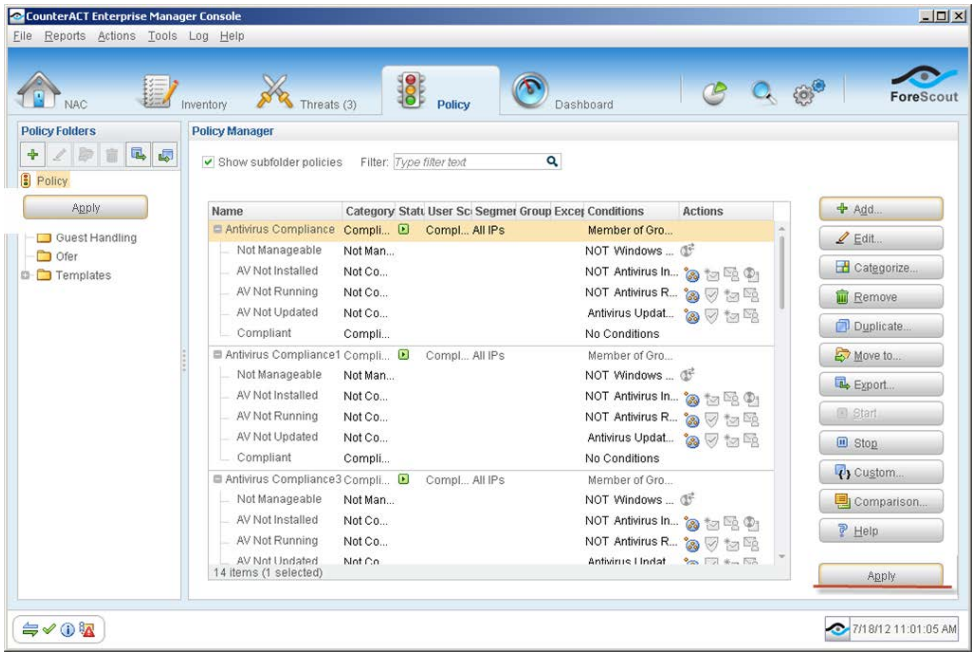
- Antivirus Not Installed
- Antivirus Not Running
- Antivirus Not Updated

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.

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

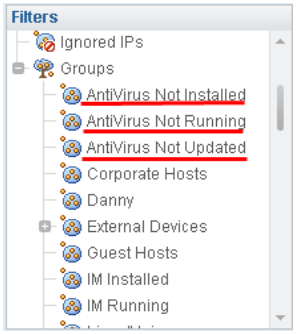
6 Activate the Policy

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.

   CounterACT detects Antivirus applications that are either not installed, not running or have not been updated.
5. On the Console toolbar, select the NAC tab.
6. In the Filters pane, expand the **Groups** folder and scroll to view the detected AntiVirus groups.



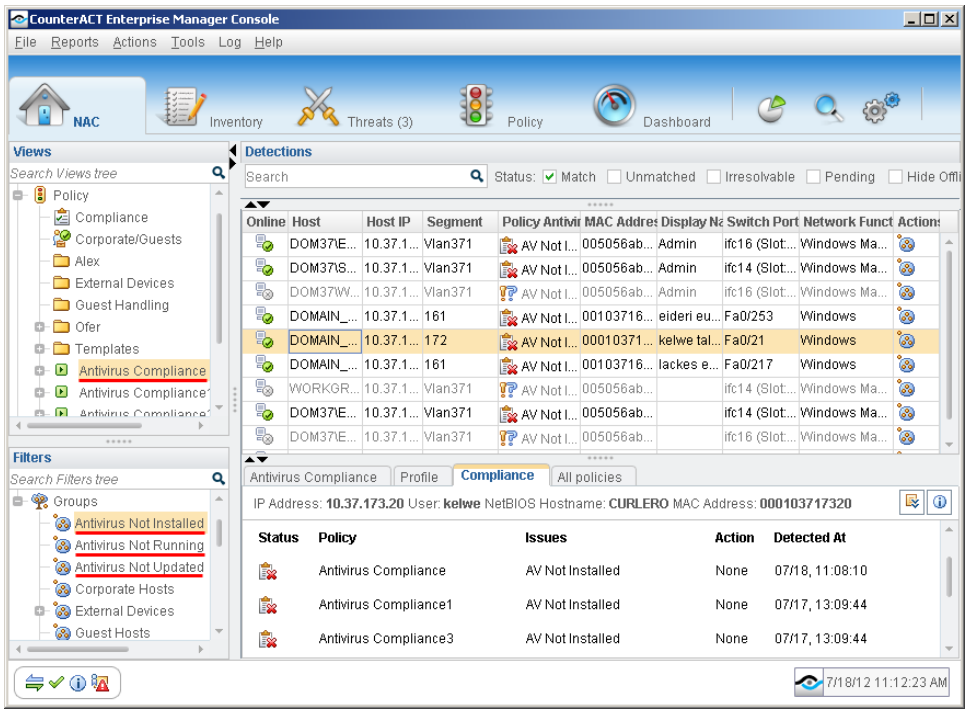
Evaluate Host Compliance

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 NAC tab.

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

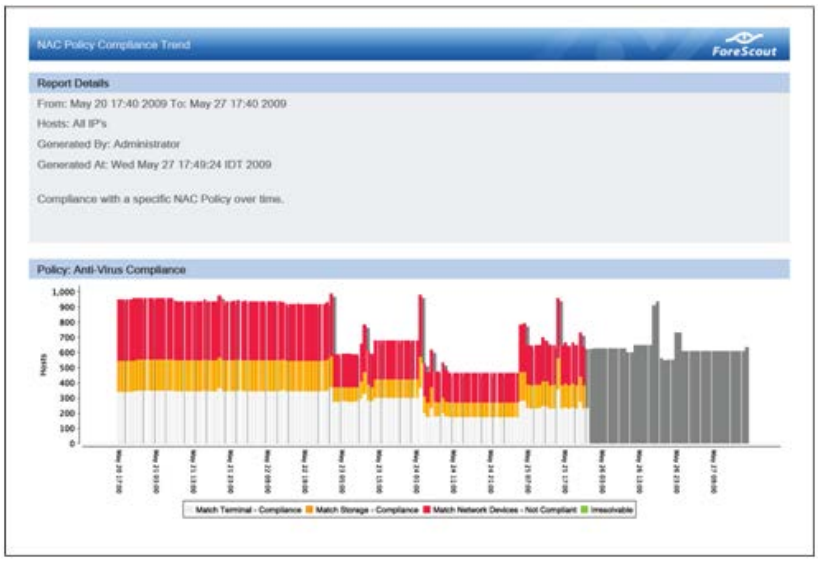
After the policy runs, you can generate reports with real-time and trend information about non-compliant hosts. You can generate and view the reports immediately, or generate schedules to ensure that Antivirus compliance is automatically and consistently reported.

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 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.



Legal Notice

Send comments and questions about this document to: documentation@forescout.com

January 2015