Ensure Instant Messaging and Peer to Peer Compliance

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Ensuring Instant Messaging and Peer to Peer Compliance

CounterACT provides powerful tools that let you continuously track and control devices where unauthorized Instant Messaging and Peer to Peer (IM/P2P) installations are detected.

Use these tools to view non-compliant host/user details, apply automated remediation measures or enable self-remediation by endpoint users.

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

- Use a wizard-based CounterACT template to create an IM/P2P Compliance policy that detects endpoints that have installed or are running these applications.
- Review an extensive range of information about each device and about the users connected to them.
- Generate real-time and trend reports on IM/P2P network compliance.

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.

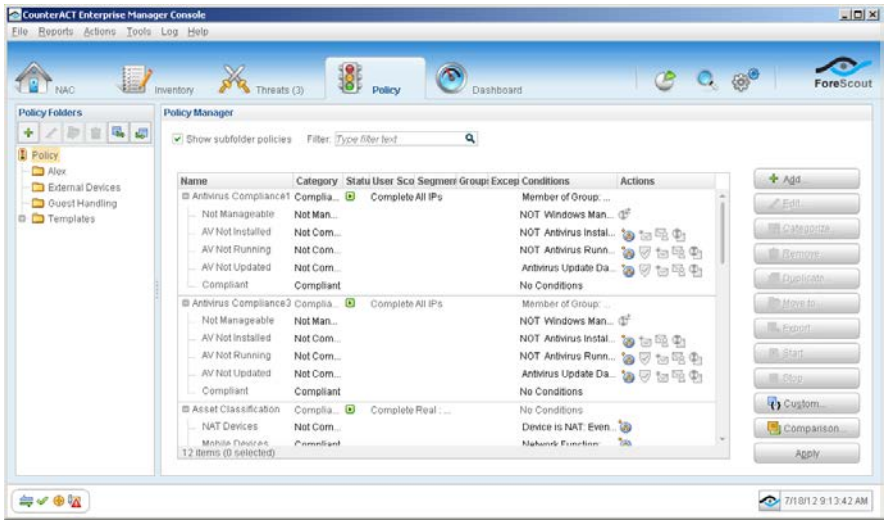
Create and Apply an IM/P2P Policy

Follow these steps to detect endpoints installing or running IM/P2P applications using a policy template.

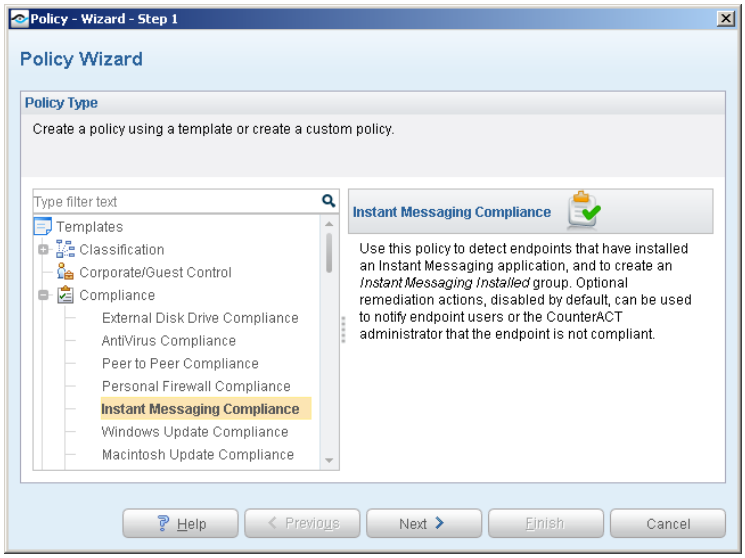
The tools used to manage IM and P2P applications are identical. This guide discusses IM applications specifically, but it also applies to P2P applications.

Select the Compliance Template

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



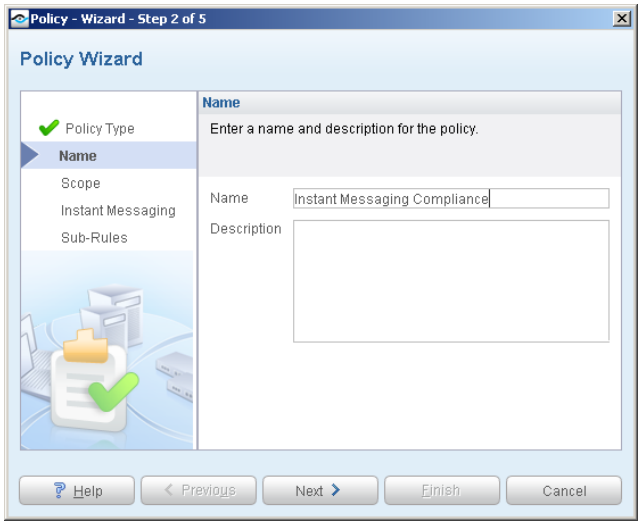
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Compliance** folder and select **Instant Messaging Compliance** (or **Peer-to-peer Compliance**).



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

Name the Policy

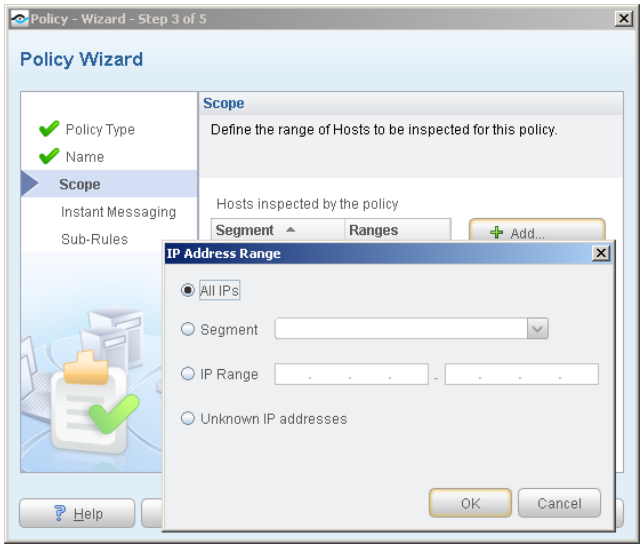
1. In the Name pane, a default policy name appears in the **Name** field.



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 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:

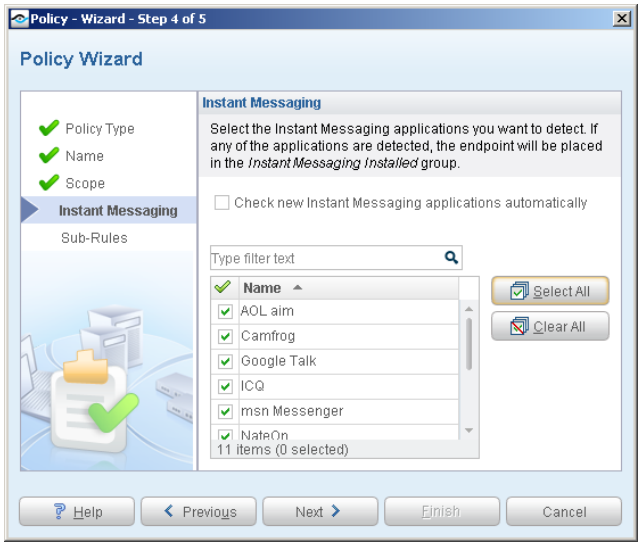
- **All IPs** lets you inspect all addresses in the Internal Network range, initially defined when CounterACT was set up.
- **Segment** lets you select a previously defined segment of the network. To specify multiple segments, select **Cancel** to close the IP address range dialog box, and select **Segments** 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 Instant Messaging (or Peer-to-peer) pane opens.

4 Choose Vendors to Manage

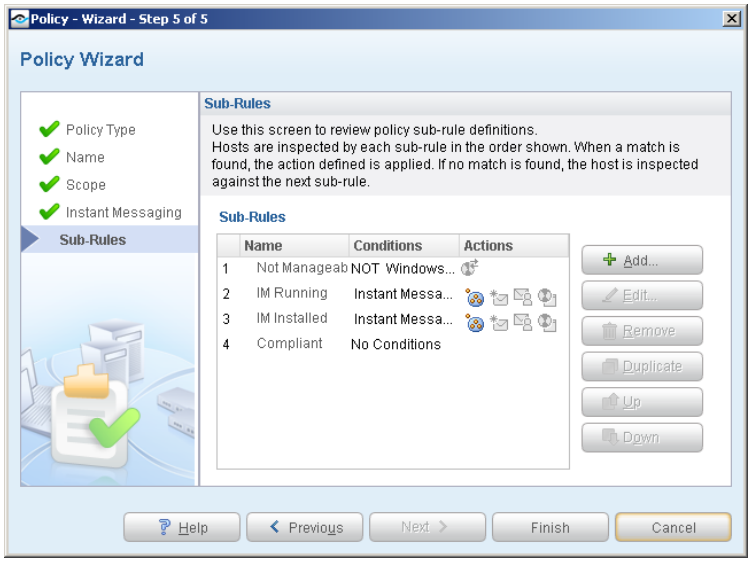
1. Select the checkboxes of specific vendors to detect, or select **Select All**.



2. New vendors may be added to this list in between CounterACT version releases. To automatically include newly supported vendors/versions in the inspection, select the **Check new Instant Messaging applications automatically** checkbox.
3. Select **Next**. The Sub-Rules pane opens.

5 Finish Policy Creation

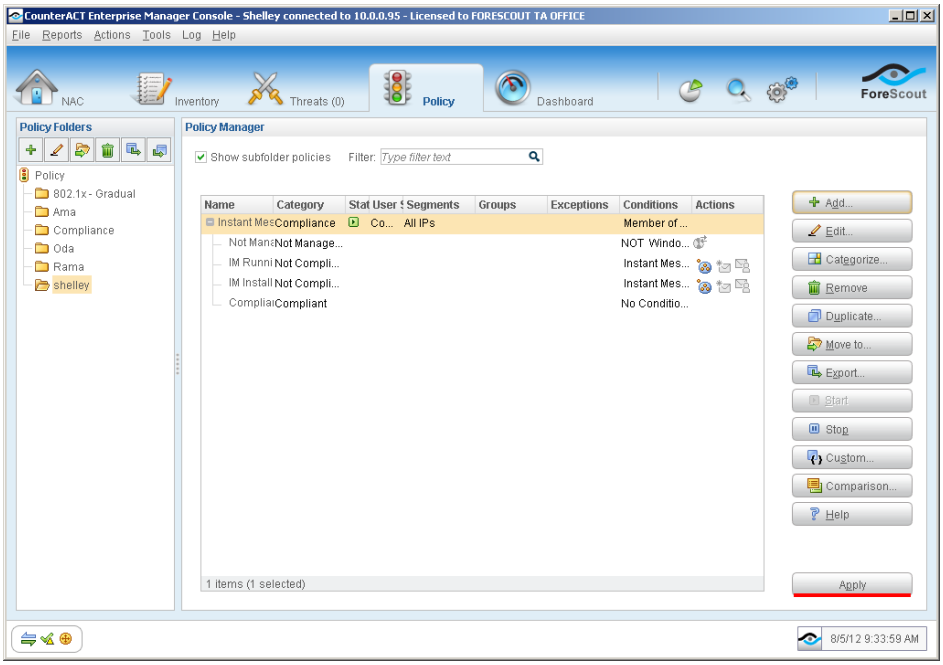
The policy sub-rules are displayed in the Sub-Rules pane. Rules instruct CounterACT how to detect hosts (Conditions) and handle hosts (Actions). The *Add to Group* action is enabled by default. Optional remediation actions, disabled by default, can be used to notify endpoint users or the CounterACT administrator that the endpoint is not compliant. 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.

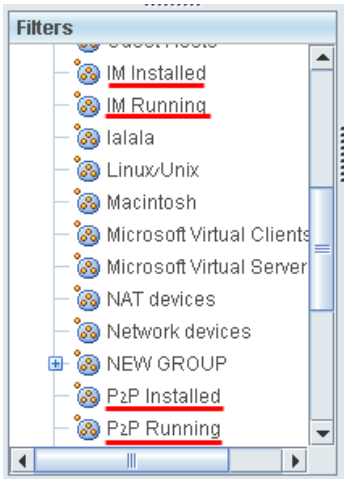
6 Activate the Policy

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 open. Select **Yes** or **OK** accordingly. On completion, the policy is activated.

   CounterACT detects the endpoints on which IM applications are either installed or running.
5. On the Console toolbar, select the NAC tab.
6. In the Filters pane, expand the **Groups** folder and scroll to view the detected endpoints (IM or P2P).

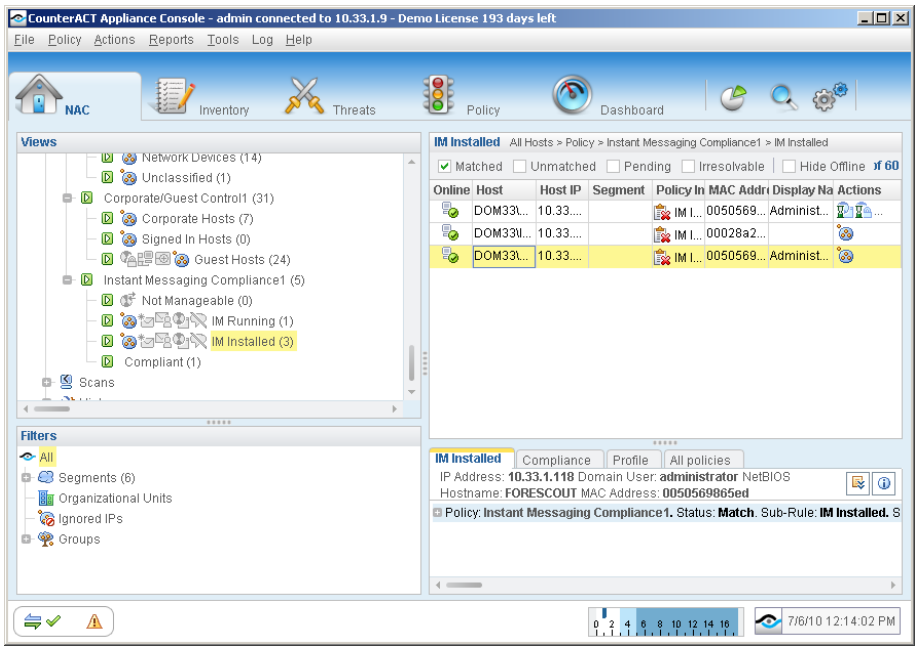


Evaluate Host Compliance

After activating the policy, you can view an extensive range of details about non-compliant endpoints and users.

To view details about non-compliant endpoints and users:

1. On the Console toolbar, select the NAC tab.
2. In the Views pane, expand the **Policy** folder and scroll to the policy you created.
3. In the Detections pane, select a host. Host information is displayed in the Details pane.



4. To customize the information displayed about hosts and users connected to endpoints, 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

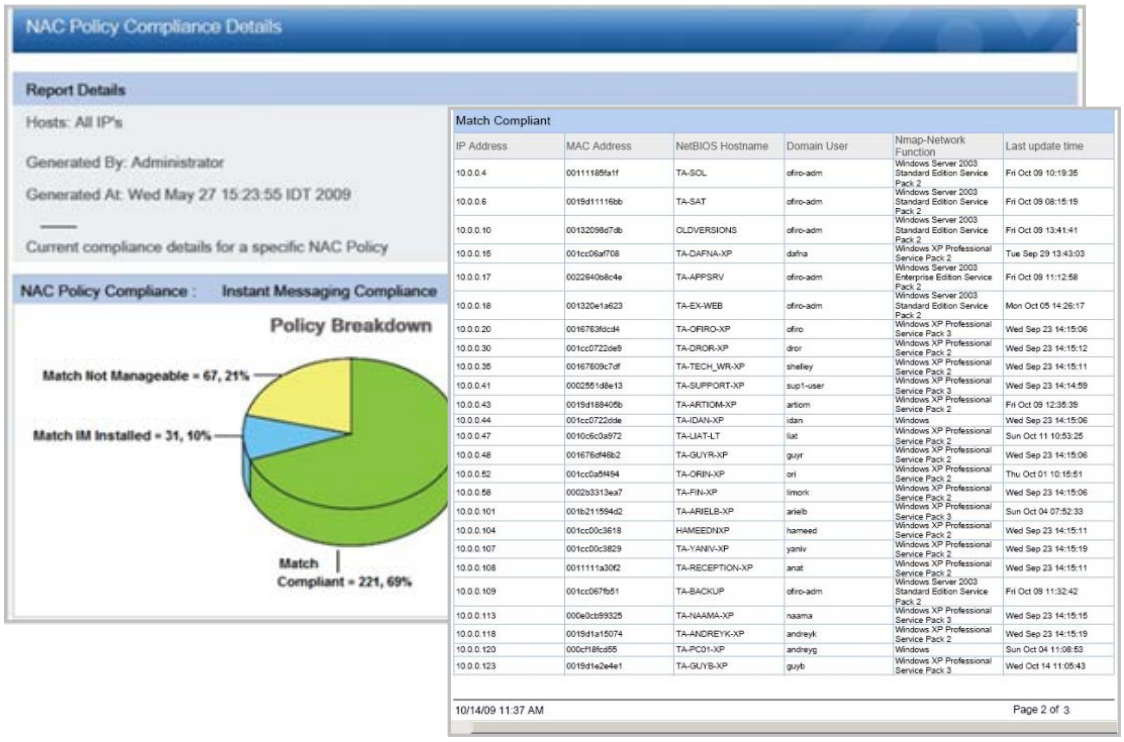
After the policy runs, you can generate reports with real-time and trend information about non-compliant hosts. You can generate and view the reports immediately, or generate schedules to ensure that changes are automatically and consistently reported.

The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User Guide.

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 a 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 Details report was selected. This report gives you a pie chart breakdown of compliance with an IM or P2P policy, and provides details depending on the information fields you selected to view.



Legal Notice

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

January 2015