Use the Executive Dashboard

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Using the Executive Dashboard

CounterACT's Executive Dashboard is a powerful web-based information center. It delivers a dynamic, real-time summary of critical activity on your network, based on information collected by CounterACT policies.

Setting Up CounterACT to Work with the Executive Dashboard

Make sure that you have met the following requirements to enable the Executive Dashboard to run properly:

- You are working with Internet Explorer version 6 or above, or Firefox version 2 or above.
- Flash 8 or above is installed on your machine.
- JavaScript is enabled on browsers running the Executive Dashboard.
- The policies you work with in the Executive Dashboard have been defined to include All IPs.
- You have run the following CounterACT templates in this order:
  - Asset Classification
  - Corporate/Guest Control
  - one or more of the Compliance templates
- You have created organizational units and assigned segments to them; for example, a Sales Organizational Unit including East, West and Central Sales Segments. The Compliance Trend and Organizational Unit Compliance graphs in the Executive Dashboard are sorted according to these units. For instructions on how to create organizational units, see Create Organizational Units.
- You have categorized and labeled the policies that you want the Executive Dashboard to include in its results. For instructions on how to categorize and label policies, see Categorize and Label Policies.

Accessing the Executive Dashboard

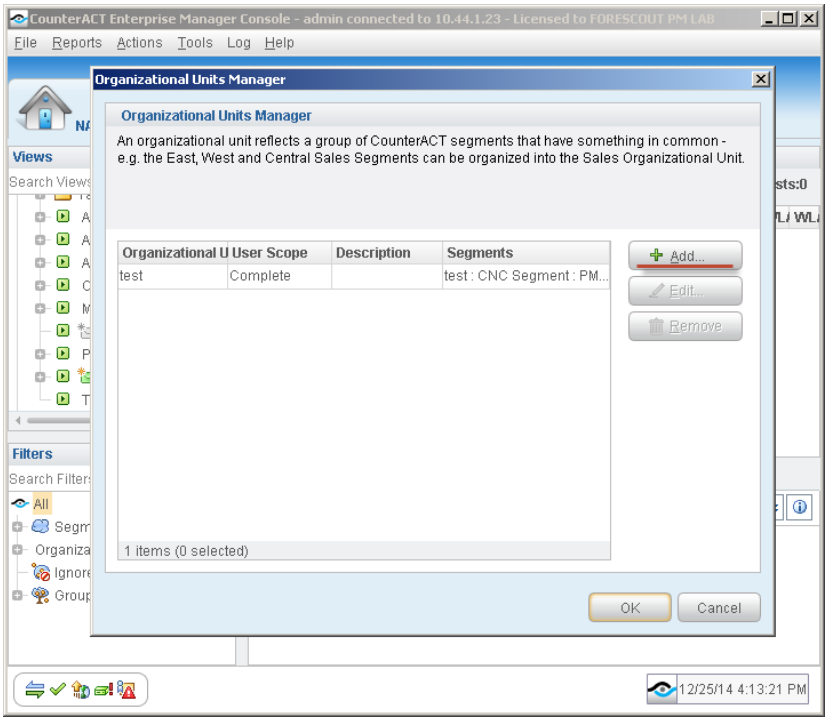
To access the Executive Dashboard:

1. Log into the CounterACT Console.
2. On the Console toolbar select the Dashboard tab. The Executive Dashboard tab opens.

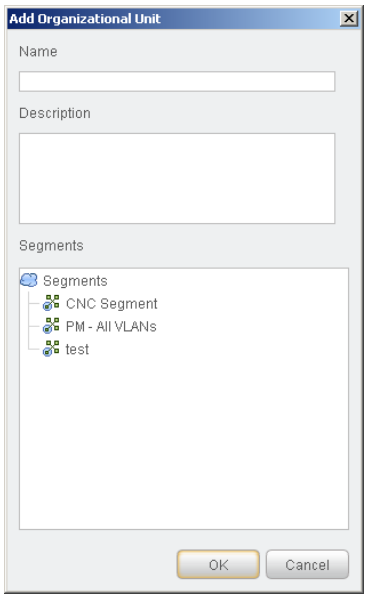
Create Organizational Units

To create organizational units:

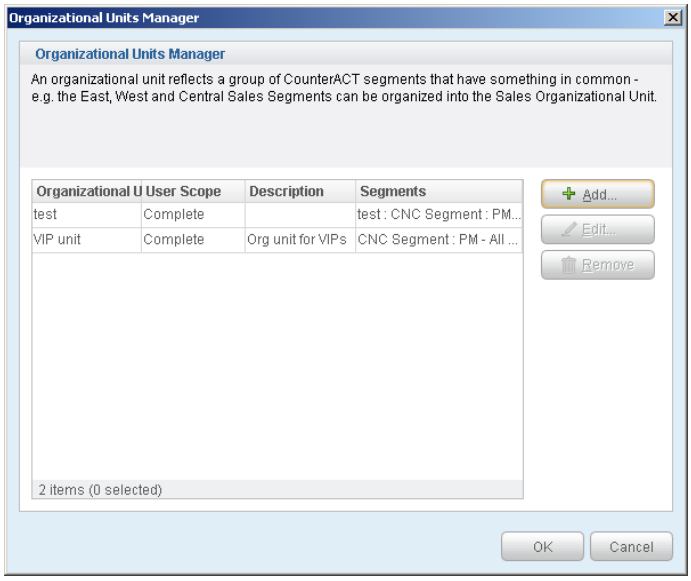
1. Log into the CounterACT Console.
2. In the Filters pane, double-click **Organizational Units**. The Organizational Units Manager opens.



3. Select **Add**. The Add Organizational Unit dialog box opens.



4. Enter a name and description (optional) for the organizational unit, select at least one segment, and select **OK**. The information is displayed in the Organizational Units Manager.



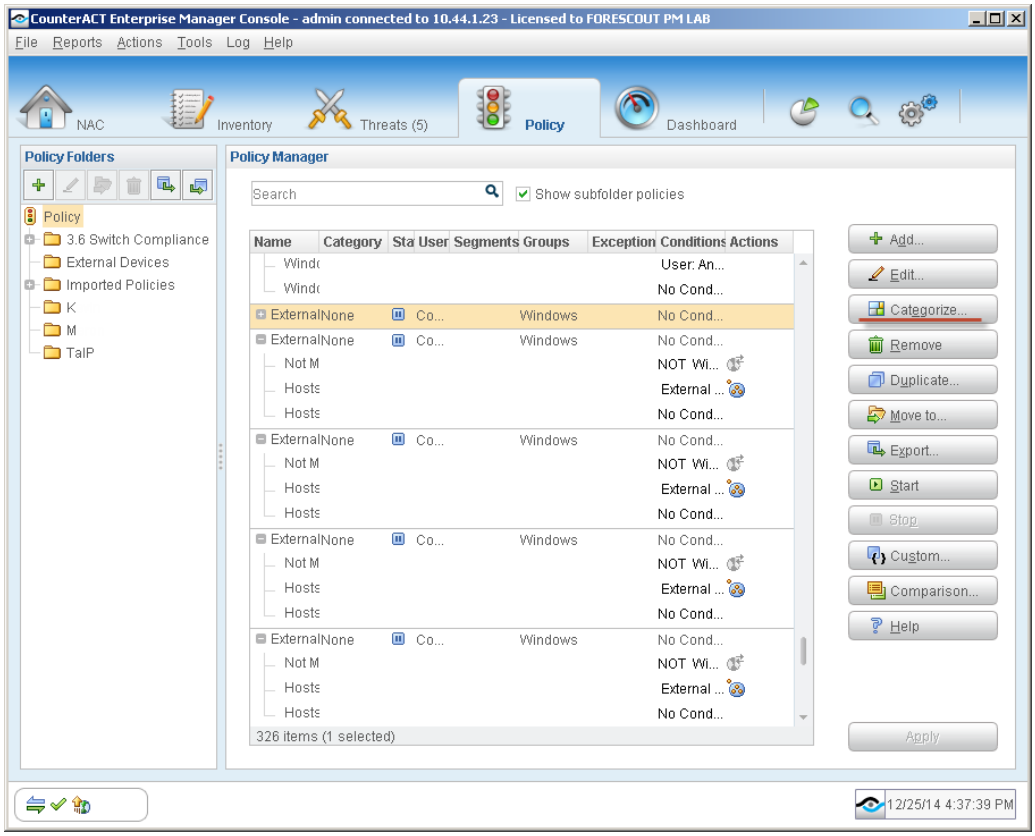
5. Select **OK** and select **Yes** to save the changes.

For more information on the extended configuration options, refer to the Console User Manual or the Console Online Help.

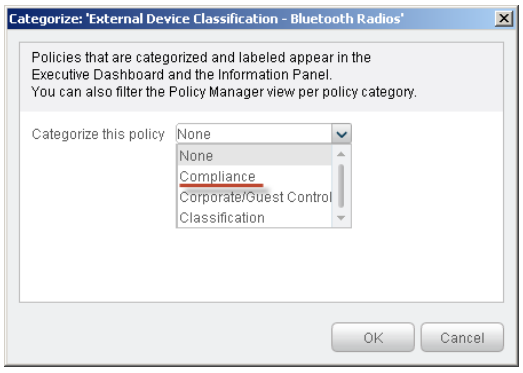
Categorize and Label Policies

To categorize and label policies:

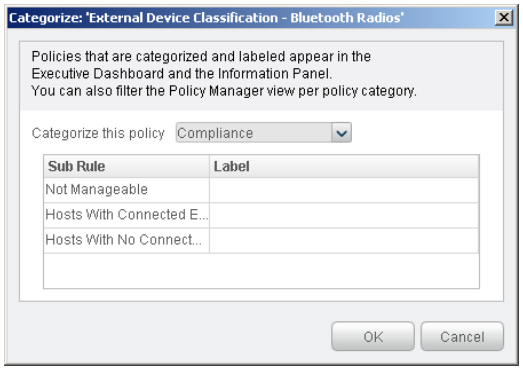
1. Log into the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.



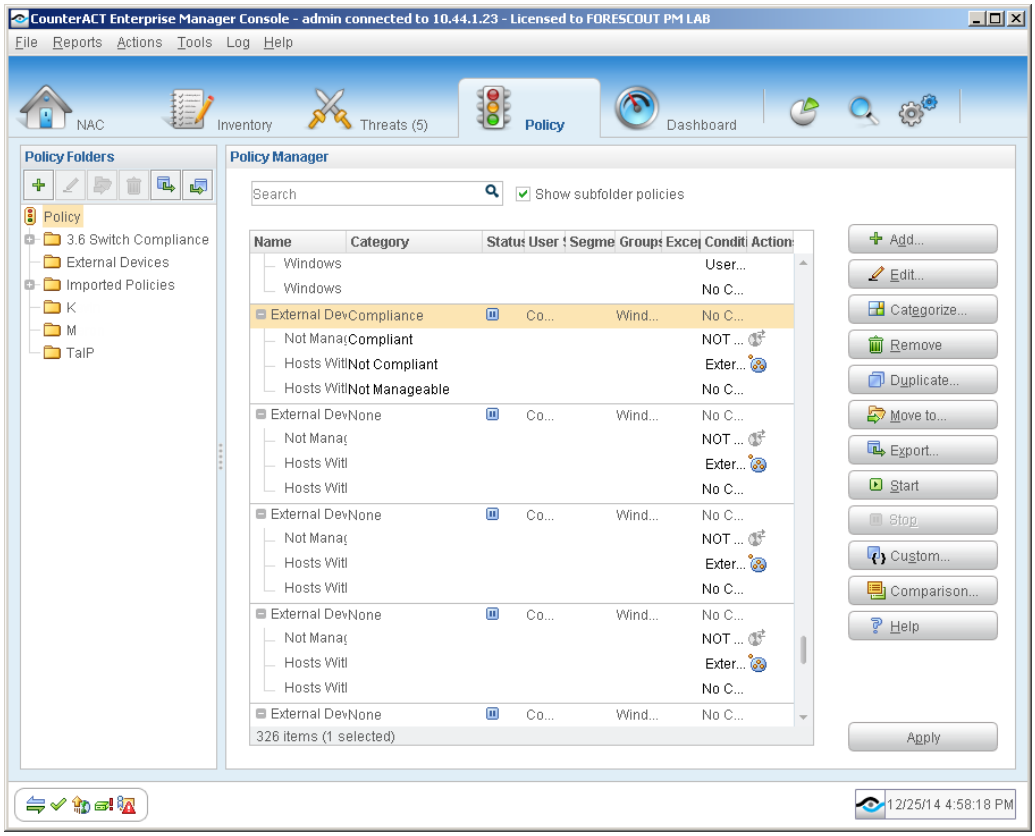
3. Select a policy and then select the **Categorize** button. The Categorize dialog box opens.



4. Select the **Compliance** option from the drop-down list.



5. For each sub-rule, select a label from the drop-down list.
6. Select **OK**. The compliance settings are displayed in the Policy Manager.



7. Select **Apply**.

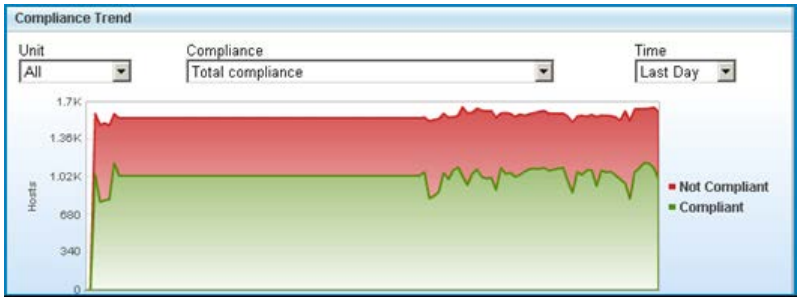
For more information on the extended configuration options, refer to the Console User Manual or the Console Online Help.

A Close-Up Look at the Executive Dashboard

The Executive Dashboard is divided into six sections.

1 Compliance Trend

This section displays compliance trends for specified organizational units in your enterprise.

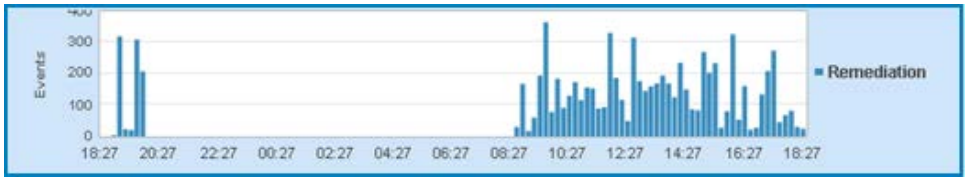


For example, you can display the number of endpoints in the sales department that used/did not use unauthorized Instant Messaging applications over the last month. Hosts that meet Total Compliance match at least one compliance requirement, and do not match any non-compliance requirements. If a host matches a compliance policy but is unlabeled for other policies, it is considered totally compliant.

From the drop-down lists, select an organizational unit, a compliance policy and a time period. Use the tooltip when hovering over the graph line to view information on how many hosts were or were not compliant at any given time.

2 Remediation Trend

This section displays information about the number of remediated events over a given time period for the selected policies and organizational units.



Remediation occurs when the host status changes from *non-compliant* to *compliant*; for example, hosts that used unauthorized Instant Messaging applications and then uninstalled them.

3 Real-time Organizational Unit Compliance

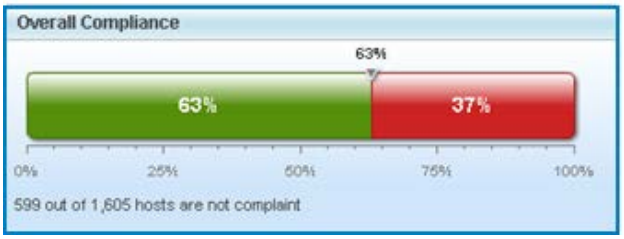
This section shows real-time policy compliance statistics for organizational units in your enterprise.

Hosts that meet Total Compliance match at least one compliance requirement, and do not match any non-compliance requirements. If a host matches a compliance policy but is unlabeled for other policies, it is considered totally compliant.

Select from the drop-down list to display organizational unit information for specific compliance policies or for all policies (Total compliance). Hover over the bars of the table to show the equivalent percentage.

4 Real-time Overall Network Compliance

This section displays both the percentage and the number of compliant versus non-compliant hosts in your network.



5 Gauges

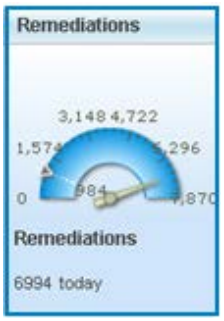
Dashboard gauges provide information about network guests, malicious hosts and remediation events.

The gauges for network guests and malicious hosts indicate:

- Gauge needle: real-time detection information.
- Gauge line and number: weekly average.
- Numerical values: weekly range.

For remediation events, the gauge indicates different information. See Remediations.

Guests



Authorized Guests are hosts that are not part of your domain but were authorized to access your internal network, such as the laptop used by an outside contractor who authenticated to the network with the right credentials.
Unauthorized Guests are hosts that did not properly authenticate.

You can decide which matched rules should be labeled to create *Authorized* and *Unauthorized Guests*.

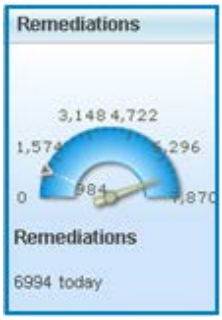
Threats

The Threats gauge indicates how many hosts are maliciously scanning or attempting to infect your network. These hosts are detected via the Threat Protection Policy.

Blocked indicates how many endpoints have been blocked by CounterACT after detecting malicious activity. If this number is “0”, you may need to change your Threat Protection Policy from Monitor mode to Block mode.

Monitored indicates the total number of machines that are being tracked as potential threats but are not blocked. If this number is “0”, you may need to change your Threat Protection Policy from Block mode to Monitor mode.

Remediation



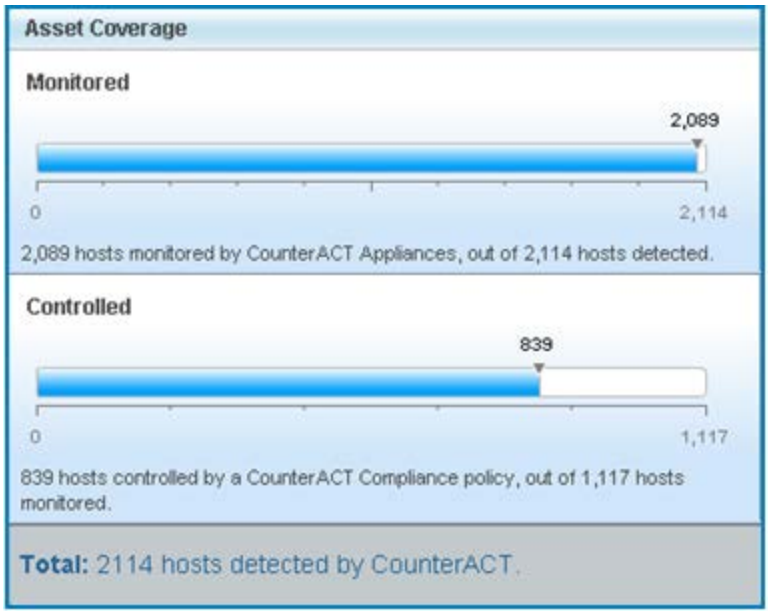
A remediation event occurs when the host status changes from *non-compliant* to *compliant*. For example, a remediation event occurs if a CounterACT policy detects that a host installed an unauthorized application and later detects that it was removed. Results are displayed on a daily basis starting from midnight.

The gauge indicates:

- Gauge needle: number of remediation events from 12:00AM until the current time.
- Gauge line and number: average of daily remediation events.
- Numerical values: number of daily remediation events (12:00AM-11:59PM) over the last week.

6 Real-time Asset Coverage

This section displays the status of hosts within your network that are monitored by CounterACT and protected by CounterACT policies.



Monitored

This value represents the number of endpoints assigned to CounterACT Appliances for tracking.

Controlled

This value represents Windows, Macintosh and Linux endpoints monitored by CounterACT Appliances that are within the scope of addresses of at least one CounterACT policy. Other types of network devices are not included in the calculation; for example, guest hosts, printers, Virtual Machines and switches.

Total

This value represents all hosts detected by CounterACT, including hosts assigned to an Appliance as well as hosts detected by CounterACT passively but not specifically assigned to an Appliance.

- *If the number of Monitored, Controlled and Total hosts is less than the total number of devices in your network, your entire network may not be well protected. In this scenario it is advisable to broaden the scope of your policies.*

Legal Notice

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

January 2015