ForeScout

Control Corporate/Guest Hosts

How-to Guide

CounterACT Version 7.0.0

Table of Contents

About Corporate/Guest Control 3
Prerequisites 4
Create and Apply a Corporate/Guest Control Policy 4
View Registered Guests 11
Generate Reports 11

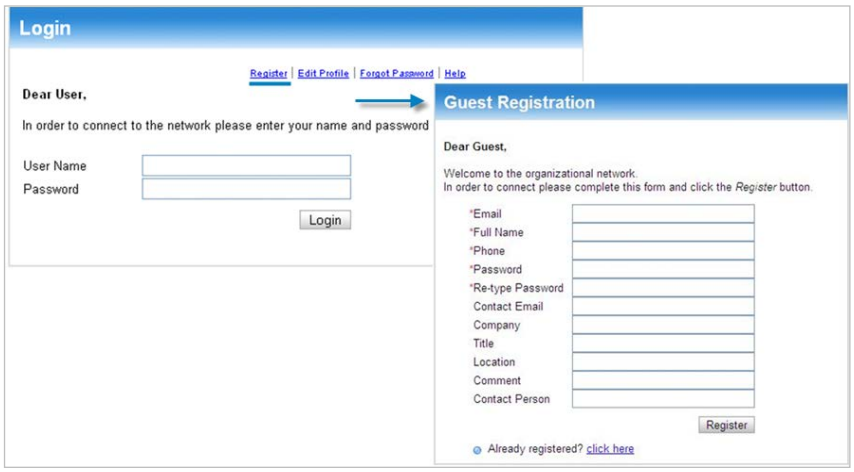
About Corporate/Guest Control

CounterACT Corporate/Guest management tools let you find and classify hosts in your network that belong to the following groups:

- Corporate Hosts
- Signed-In Guests
- Guest Hosts

CounterACT policy tools let you assign the appropriate level of network access to corporate users and guests.

Use these tools to prompt unauthorized users to register as guests, and to assign network access permissions to them. By default, the policy template is designed to prompt users at non-corporate hosts to register as network guests by entering their contact details. All hosts receive a Login page at their desktop. If the host is a guest and not a corporate user, the Guest Registration page opens.



The login request is delivered to an individual in your enterprise with the authority to approve network access. If approved, login credentials are automatically sent to the email address entered in the registration form.

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

- Use a wizard-based CounterACT template to create a Corporate/Guest Control policy that classifies and handles corporate hosts and guests.
- Review information about corporate and guest detections.
- Generate real-time reports on corporate hosts and guests.

This How-to guide provides basic configuration instructions designed for a quick setup. Other options are available for handling network guests. For example, you can pre-register users as guests or let guests skip the registration/sign in process and enter the network with limited access. For information about these options, refer to the Console Online Help.

Prerequisites

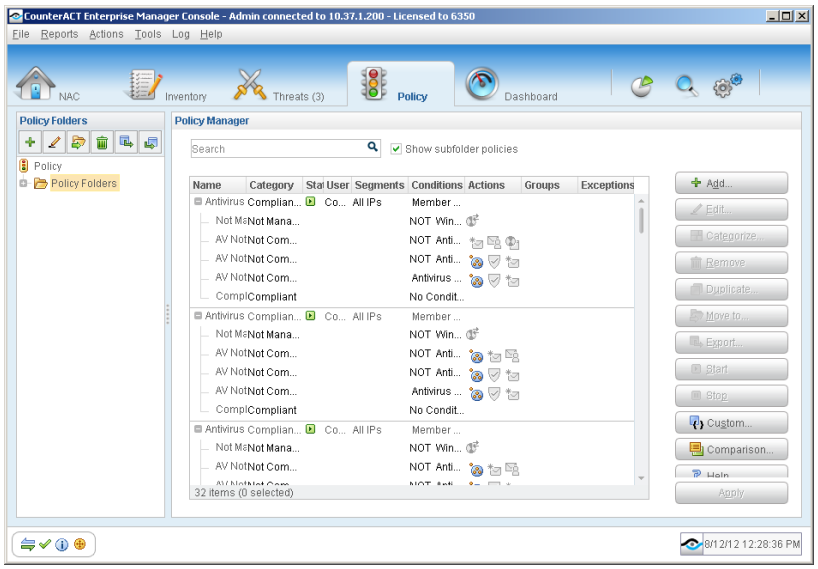
- Verify that you have run the Asset Classification template and that it is applied to the network segments or IP ranges on which you want to run the Corporate/Guest Control policy.

Create and Apply a Corporate/Guest Control Policy

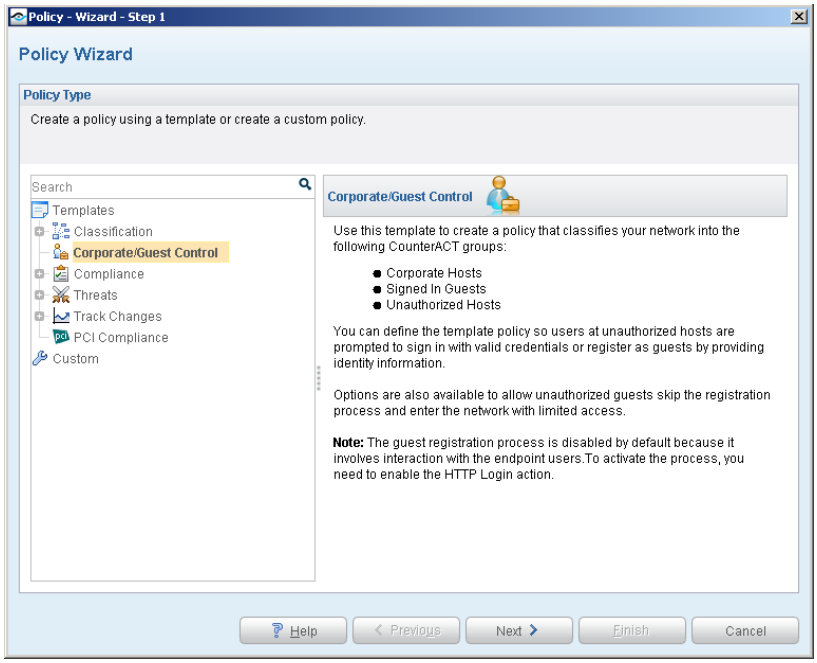
Follow these steps to detect, classify and control corporate and guest hosts using a policy template.

Select the Corporate/Guest Control Template

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



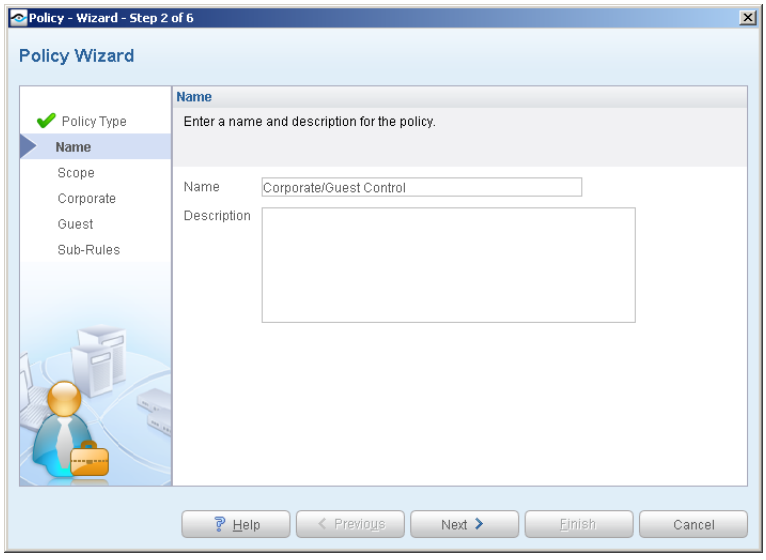
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, expand the **Classification** folder and select **Corporate/Guest Control**.



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

2 Name the Policy

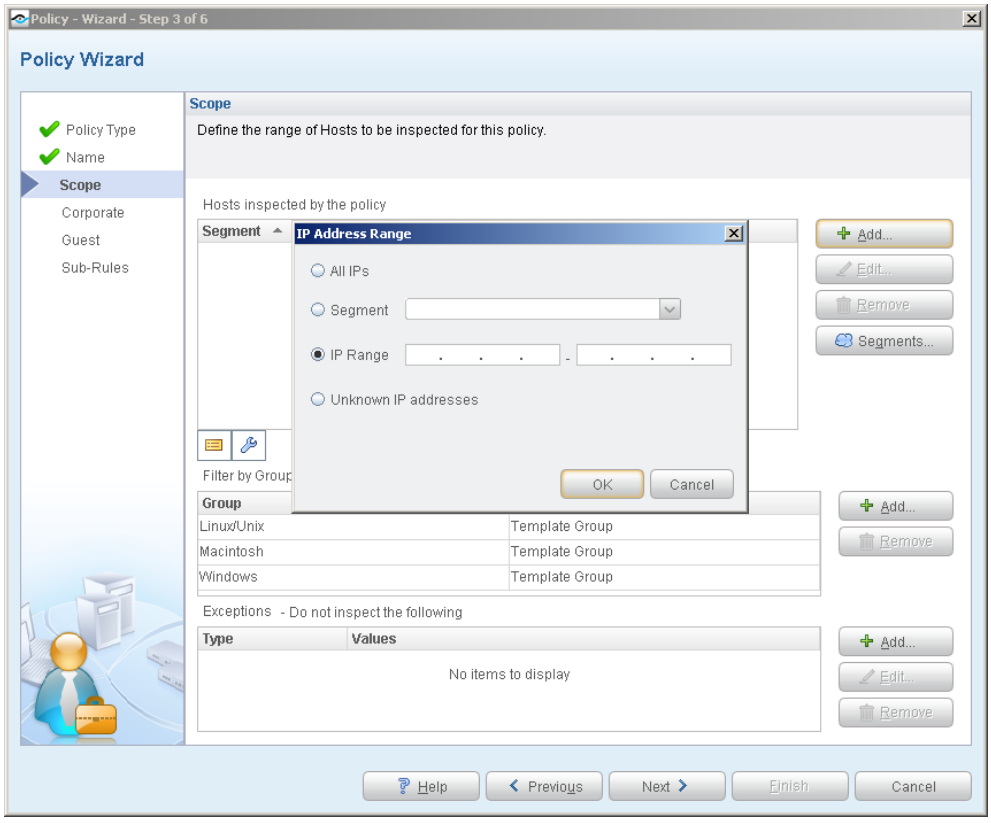
1. In the Name pane, a default policy name appears in the **Name** field.



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.

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.

   By default, the policy template includes Windows, Macintosh and Linux/Unix machines identified by the Asset Classification policy. The items appear in the *Filter by Group* section of the Scope pane.

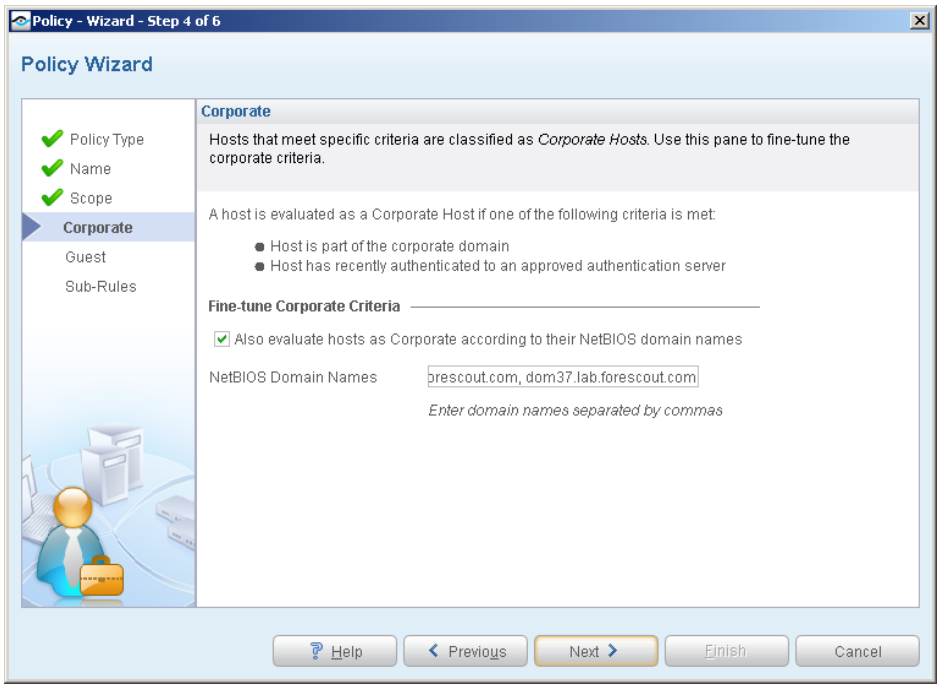
3. Select **Next**. The Corporate pane opens.

Define Corporate Host Criteria

By default, hosts automatically become members of the *Corporate Hosts* group if they belong to a corporate domain, or were recently authenticated to an approved server.

In addition, you can instruct CounterACT to classify a host as *corporate* if its NetBIOS name matches the prefix of a Fully Qualified Domain Name (FQDN). This optional criterion is typically used by organizations working with legacy systems that are not part of the Active Directory Domain, but publish a known NetBIOS domain name.

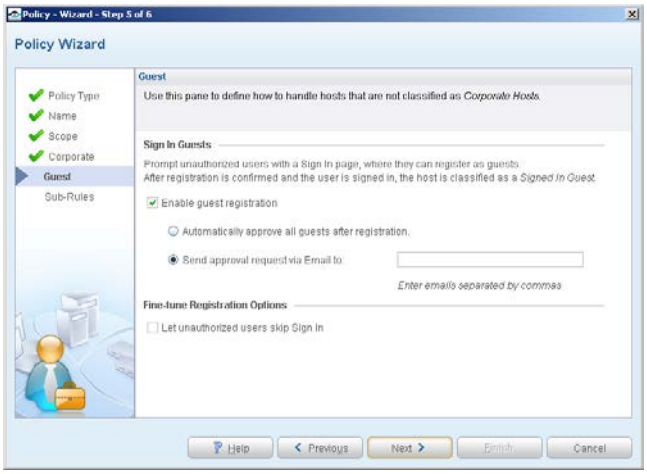
1. Enter domain names in the **NetBIOS Domain Names** field. Separate multiple domain names with commas.



2. Select **Next**. The Guest pane opens.

Define How to Handle Guests

1. In the **Sign In Guests** section, the **Enable guest registration** and **Send approval request via Email to** options are selected by default. When these options are selected, CounterACT requires guest hosts to register, and submits registration information to administrators for approval. Enter the email addresses of individuals in your enterprise who will approve these network access requests. Separate multiple emails with commas.

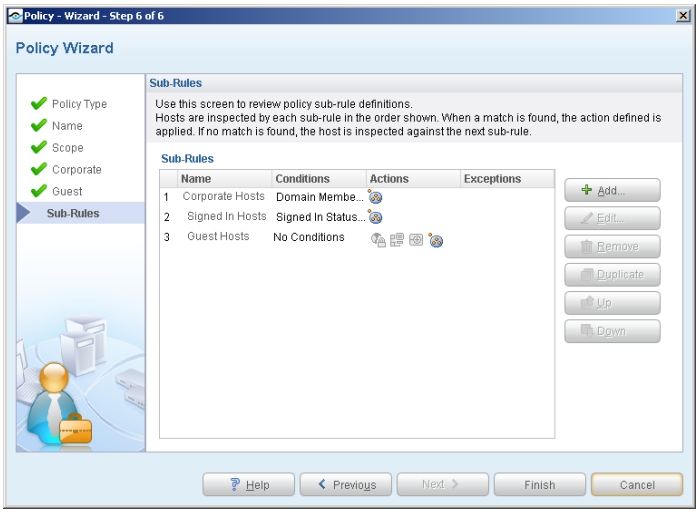


By default, the new policy does not implement guest registration. First run the policy and verify that it correctly identifies guest hosts, and then implement the registration interaction. See Implement Login and Registration Actions.

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

6 Review Sub-Rules and Finish Policy Creation

Sub-rules instruct CounterACT to inspect and handle network hosts, based on your definitions in the Scope, Corporate and Guest panes. The options defined for carrying out login and guest registration (guest screening) are disabled by default.

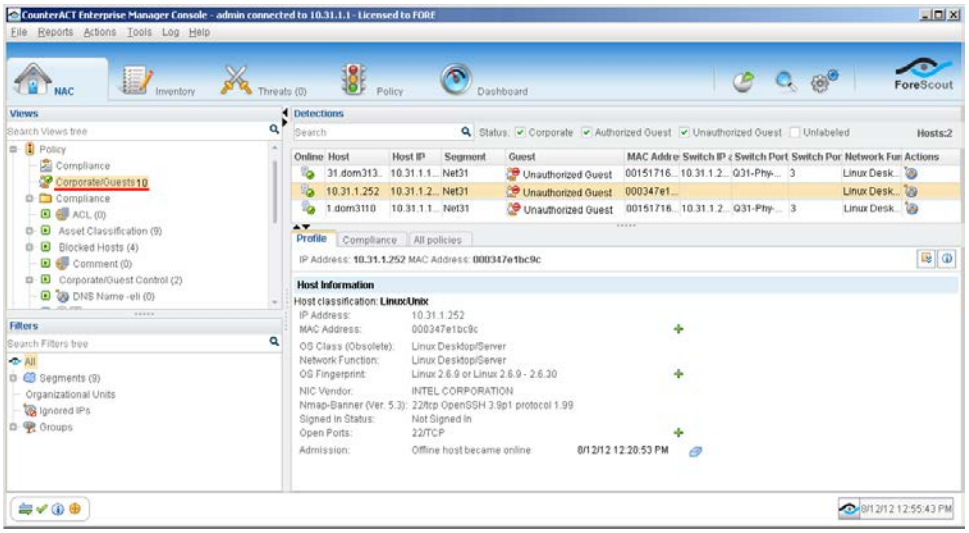


1. Select **Finish**. The policy automatically appears highlighted in the Policy Manager, where it can be activated.

7 Activate the Policy and Classify Hosts

Run the policy and review the corporate/guest groups generated by it to verify that the policy correctly identified hosts.

1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, select the policy you created, and select **Apply**. The policy is activated, and CounterACT classifies the hosts.
3. On the Console toolbar, select the NAC tab.
4. Perform one of the following:
   - In the Views pane, expand the **Policy** folder and scroll to your Corporate/Guest Control policy.
   - In the Filters pane, expand the **Groups** folder and select the **Corporate Hosts** and **Guest Hosts** groups.

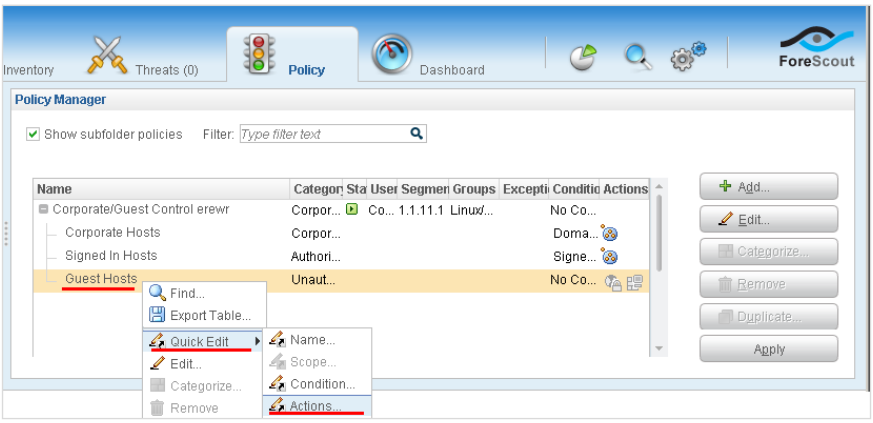


5. Verify that group membership accurately reflects your network.
6. In the Detections pane, select a host. Host information is displayed in the Details pane.
7. To customize the information displayed, right-click a column heading, select **Add/Remove Columns**, and select the information of interest to you. You can also reorder the columns.

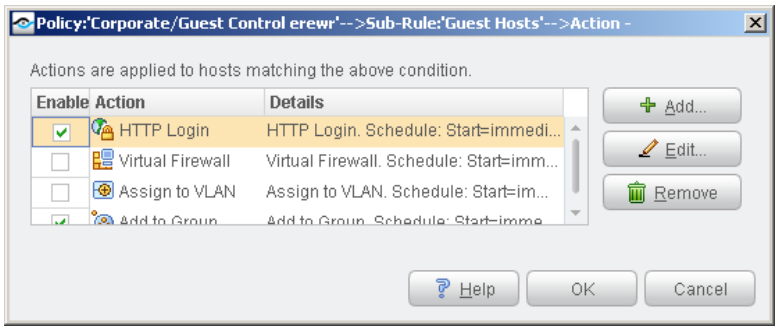
Implement Login and Registration Actions

After you verify that your policy accurately identifies guests and corporate users, you can enable policy actions that implement login and registration actions.

1. On the Console toolbar, select the Policy tab.
2. In the Policy Manager, scroll to the policy you created, and right-click the *Guest Hosts* sub-rule for this policy.
3. Select **Quick Edit** and then select **Actions**.

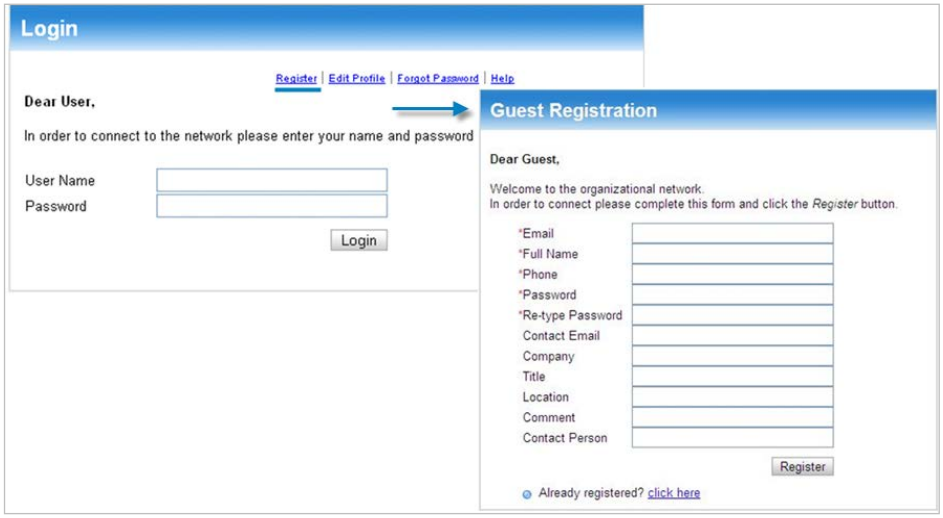


4. In the Action dialog box, enable the **HTTP Login** action.



5. Select **OK**.
6. In the Policy Manager, select **Apply**.
7. The login and guest registration actions are activated.

   During login, the guest is presented with the appropriate reqistration window.

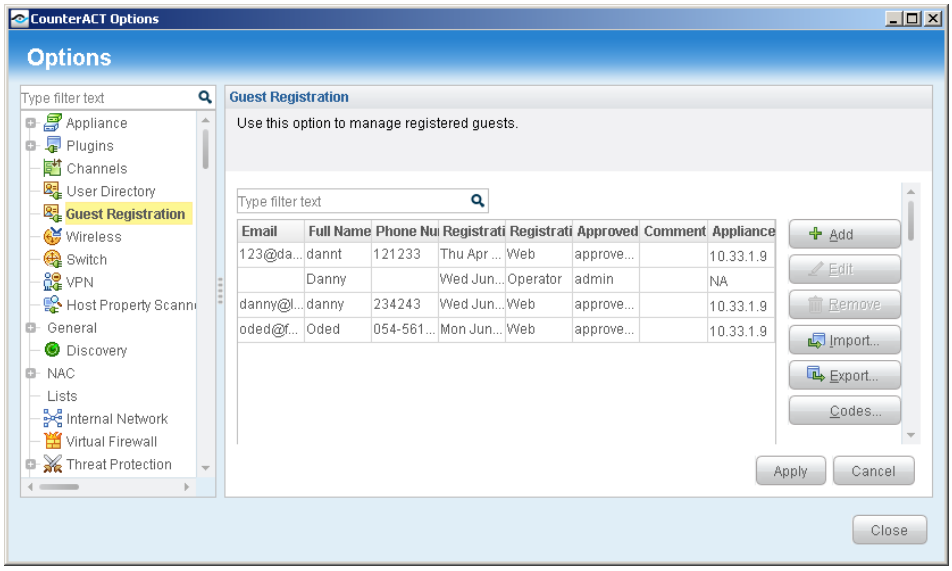


View Registered Guests

After activating the policy, you can view and edit registered guests.

To view and edit registered guests:

1. Select **Options** from the Console **Tools** menu. The Options dialog box opens.
2. Select **Guest Registration**. The Guest Registration pane opens.



3. To edit or remove a guest, select the guest.
   - If editing, select **Edit**, edit the information in the Edit Guest dialog box, and select **OK**.
   - If removing, select **Remove**.
4. Select **Apply**. The Saving User Directory Plugin Configuration dialog box opens.
5. Select **Close** twice. Login and registration tools are activated.

Generate Reports

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

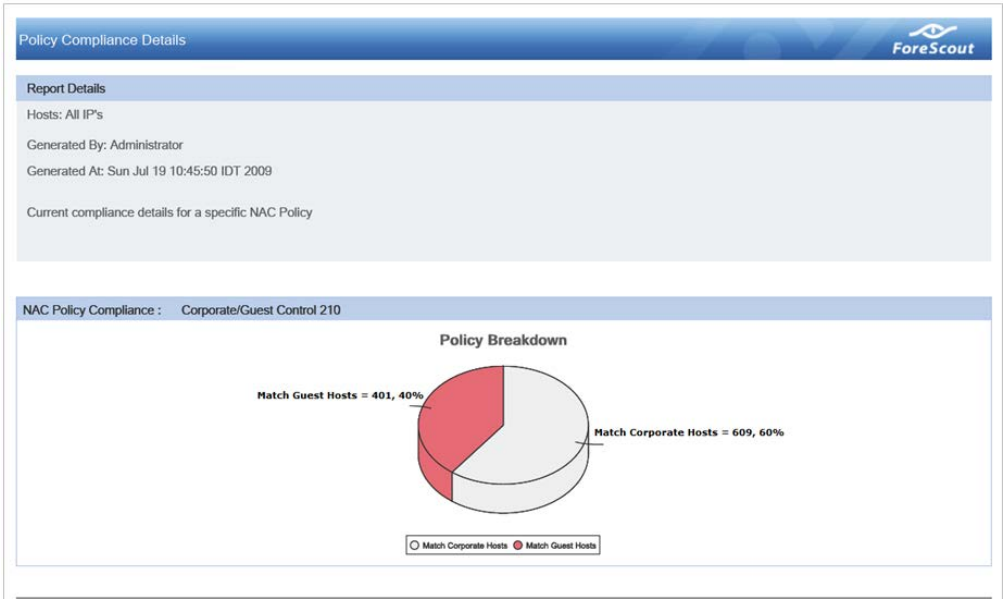
The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the CounterACT Console User Guide.

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 the Policy Trend or Policy Details 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 corporate/guest hosts, and provides details about each host depending on the information fields you selected to view.



Legal Notice

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

January 2015