ForeScout CounterACT®

Control Corporate/Guest Hosts

How-to Guide

Version 8.0

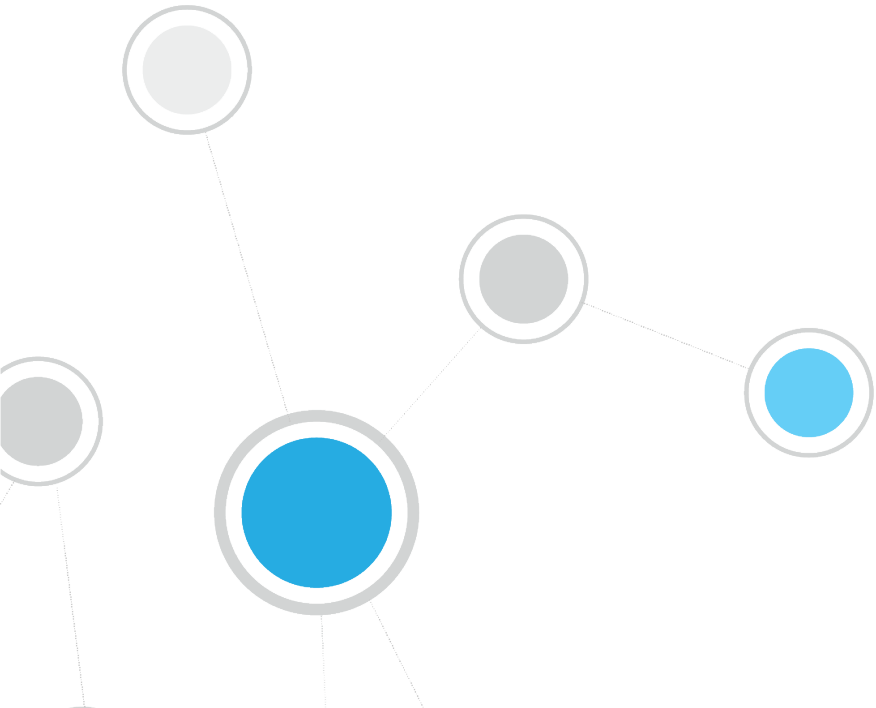


Table of Contents

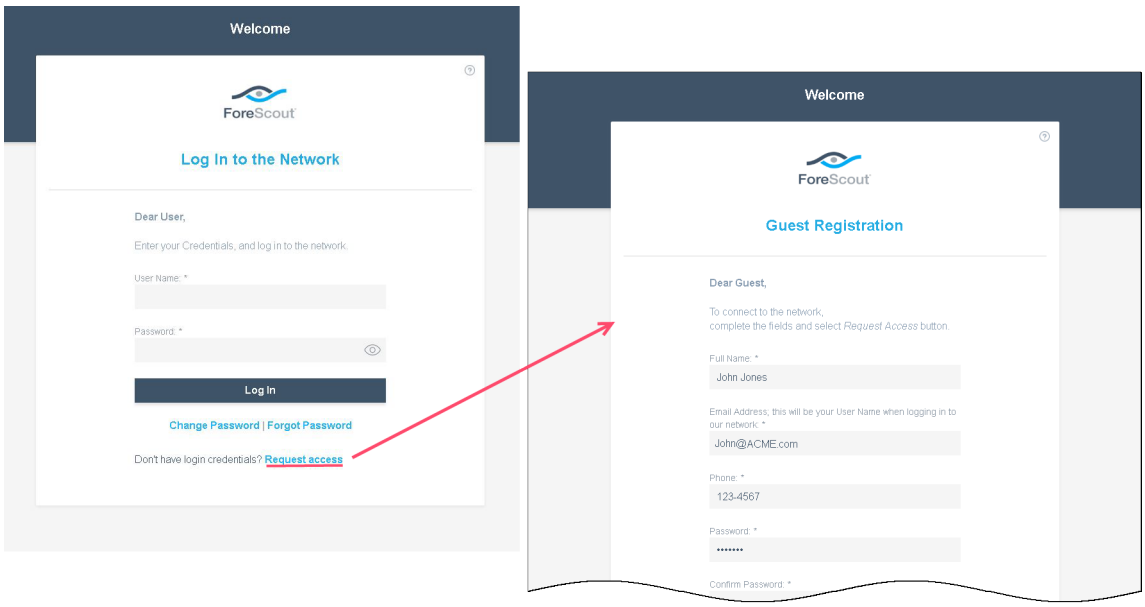
About Corporate/Guest Control

ForeScout 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 management 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 then to assign network access permissions to them. The Corporate/Guest Control policy template is designed to prompt users at non-corporate hosts to register as network guests by entering their contact details.

A Login page is displayed for all hosts. If the host is a guest and not a corporate user, the Guest Registration form opens.



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

You must set up at least one *Corporate/Guest Control* policy to trigger the detection of network guests. If you have more than one policy and want global definitions for all sponsors, verify that all the policies reflect your requirements.

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 about 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 CounterACT Administration Guide.

Prerequisites

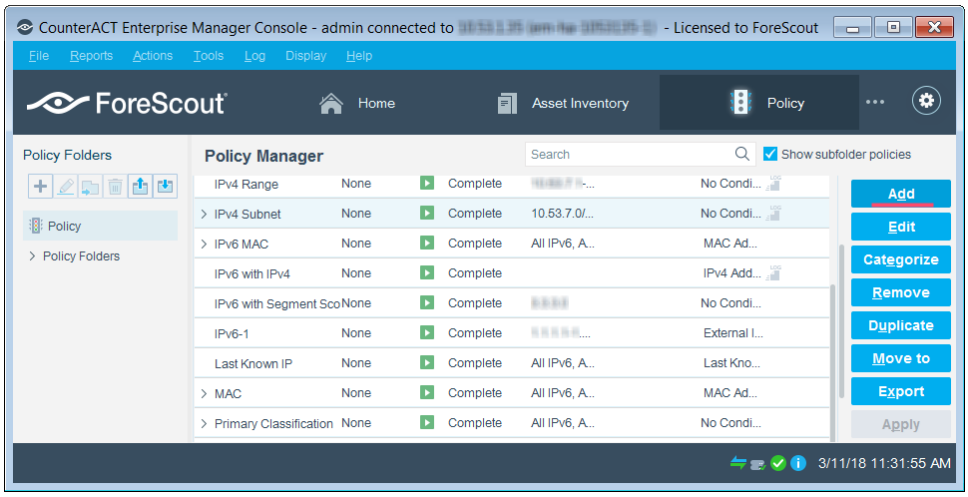
- Verify that you have run a Primary Classification or Asset Classification policy and that it is applied to the network segments or IP ranges on which you want to run the Corporate/Guest Control policy.

Create and Apply a Corporate/Guest Control Policy

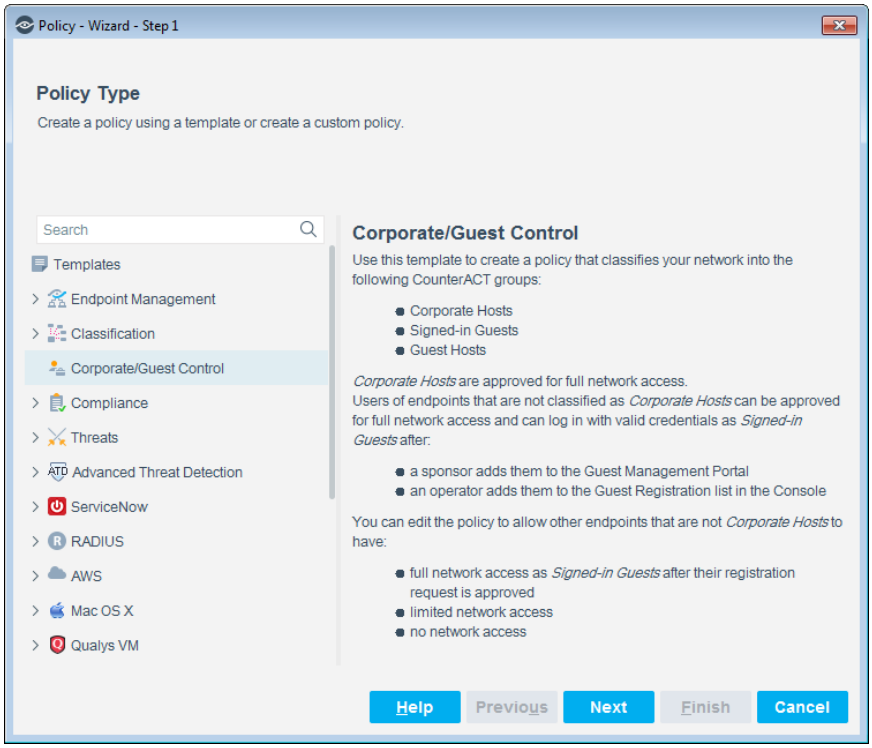
Follow these steps to detect, classify and control corporate and guest hosts using a policy template.

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.



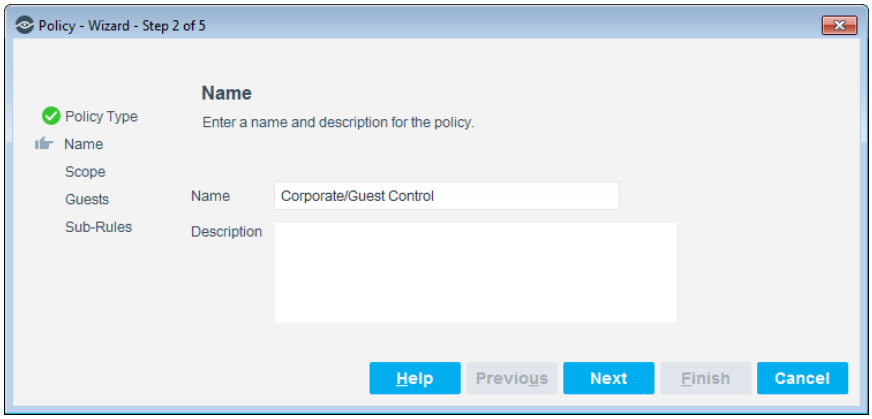
3. In the Policy Manager, select **Add**. The Policy Wizard opens, guiding you through policy creation.
4. Under **Templates**, select **Corporate/Guest Control**.



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

2 Name the Policy

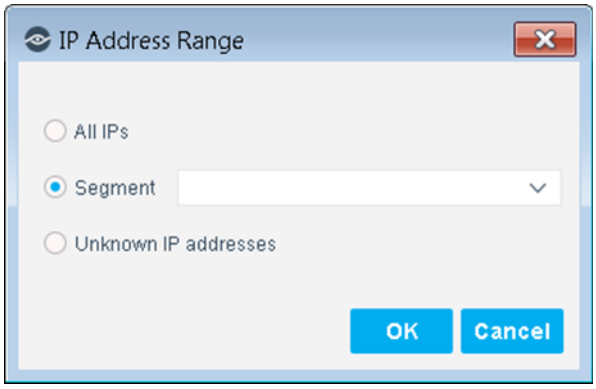
1. In the Name pane, a default policy name appears in the **Name** field.



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.

3 Choose the Hosts to Inspect

1. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

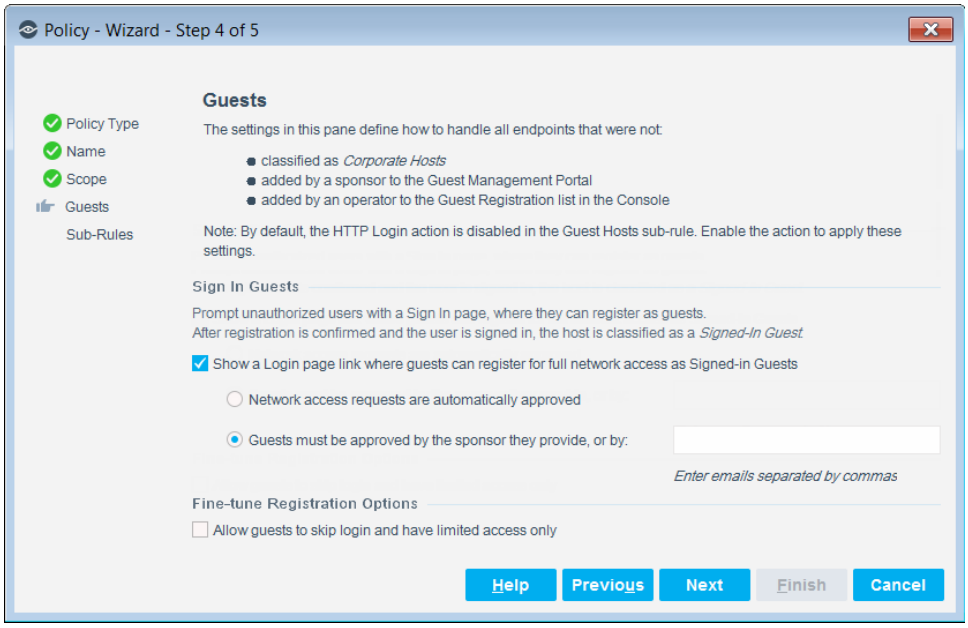
- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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 Primary Classification or Asset Classification policy. The items appear in the *Filter by Group* section of the Scope pane.

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

4 Define How to Handle Guests



1. Select the **Show a Login page link where guests can register for full network access as Signed-in Guests** checkbox to require unauthorized users not yet registered as guests to request network access using the *Guest Registration form* in a web browser.

   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.

2. To allow network access to guests upon their completion of a Guest Registration form, select **Network access requests are automatically approved**.
3. CounterACT can share the registration information submitted by guests with designated corporate contacts, called *sponsors*. Sponsors can be designated by guests in the Guest Registration form, or added in this pane. To require that a sponsor approve each guest for network access, select **Guests must be approved by the sponsor they provide, or by:**.

   Sponsor email addresses must be included in the Guest Registration, Sponsors tab.

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

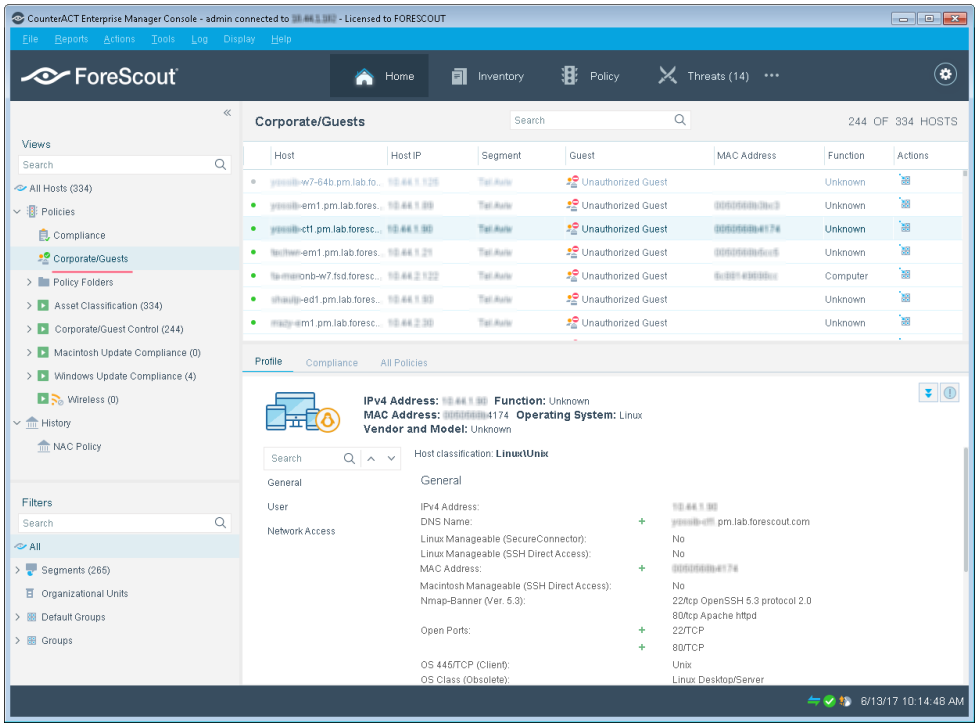
5 Review Sub-Rules and Finish Policy Creation

Sub-rules instruct CounterACT to inspect and handle network hosts, based on your definitions in the policy wizard. 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.

Activate the Policy and Classify 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 Home 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.

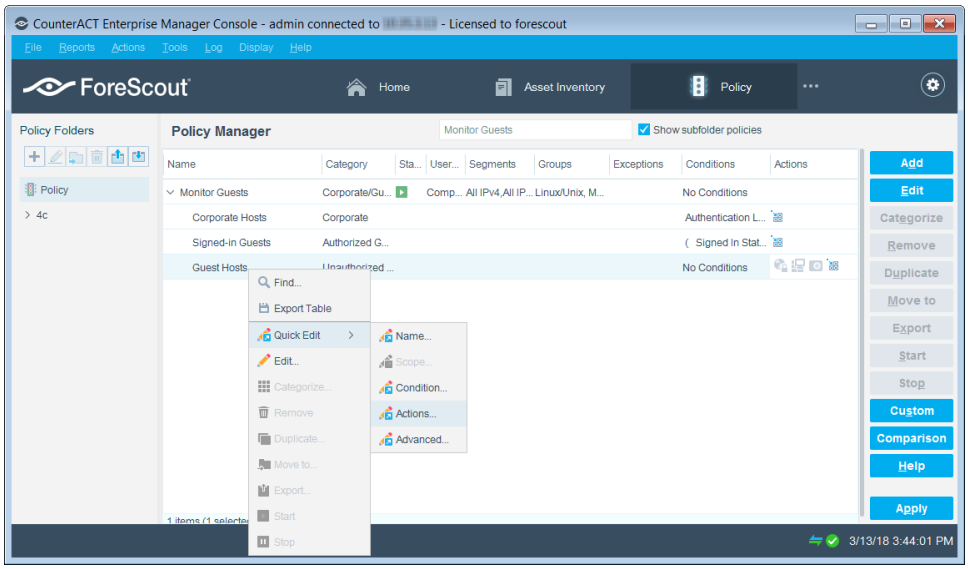


5. Verify that group membership accurately reflects your network.
6. In the Detections pane, you can select a host to see more information about it in the Details pane.
7. To customize the information displayed in the Detections pane, right-click a column heading, select **Add/Remove Columns**, and select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

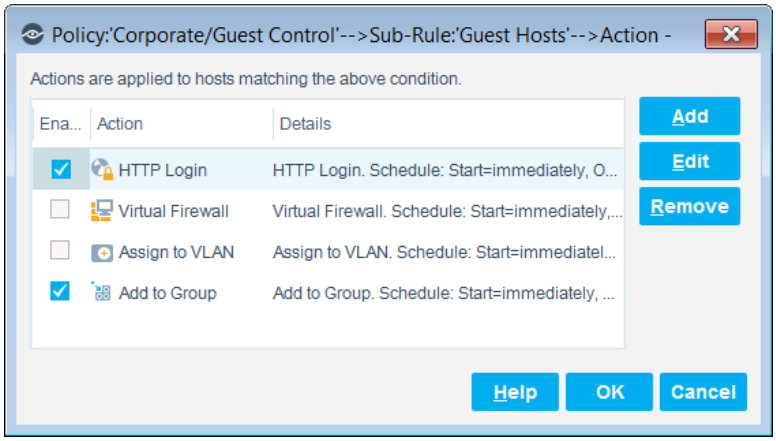
Implement Login and Registration Actions

After you verify that your policy accurately identifies guests and corporate users, you can enable policy actions that activate the Guest Registration form and other web pages or emails used for the guest registration process.

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

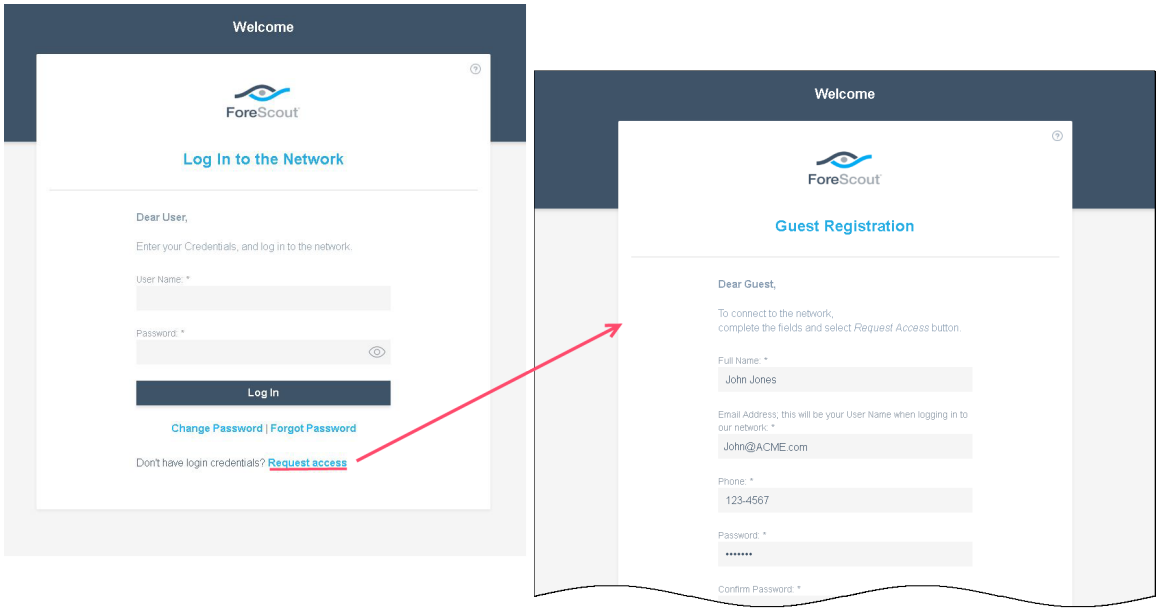


4. In the Action dialog box, enable the **HTTP Login** action.



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

During login, guests are presented with a Guest Registration form to complete.



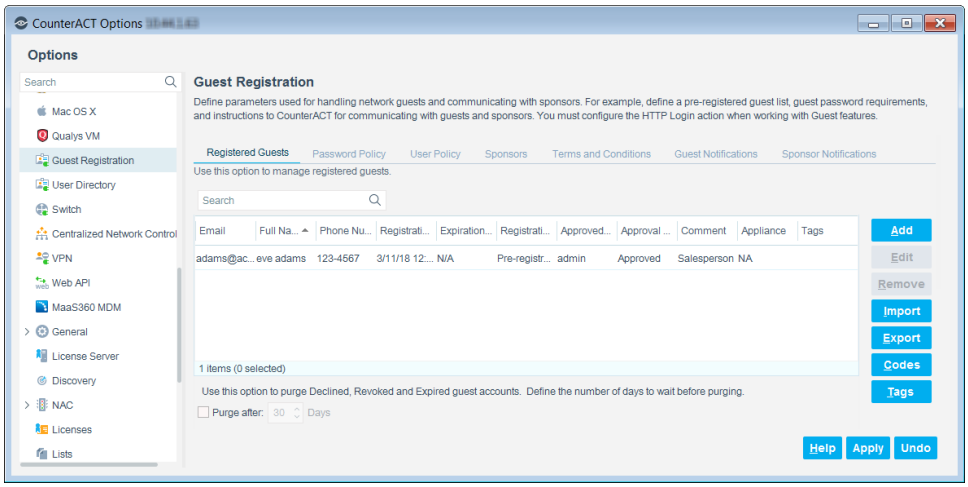
View and Manage Registered Guests

After activating the policy with the HTTP Login action, you can manage registered guests from the CounterACT Console.

Guests can also be managed from the Guest Management Portal. Refer to the Guest Management Portal for Sponsors How-to Guide. *See Additional CounterACT Documentation for information on how to access the guide.*

To manage 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 add a pre-approved guest, select **Add** and enter the guest information in the Add Guest dialog box, and select **OK**.
4. To edit or remove a guest, select the guest.
   - If editing, select **Edit**, edit the guest information in the Edit Guest dialog box, and select **OK**.
   - If removing, select **Remove**.

   Guests that you remove are automatically and immediately signed out of the network, and their accounts are purged from both CounterACT and the Guest Management Portal. Users who are removed while still browsing are notified by a web message of this management action.
5. Select **Apply**. The guest information is saved.
6. 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.

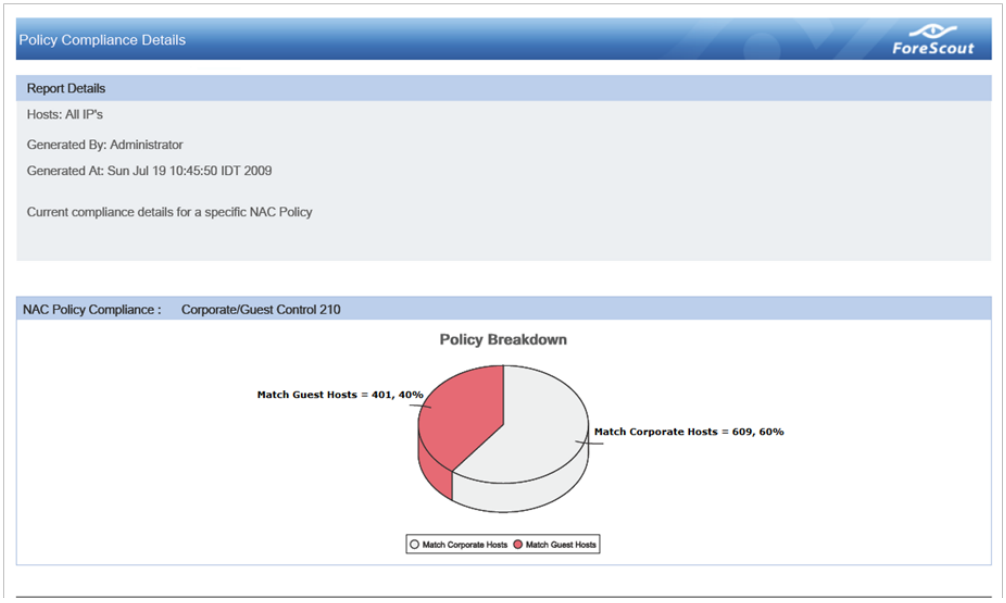
In addition, you can display and monitor the corporate and guest devices detected by the Corporate/Guest Control policy. For more information, refer to the Dashboard chapter in the CounterACT Administration Guide. See Additional CounterACT Documentation for information on how to access the guide.

The Reports Portal provides tools to customize reports and schedule automatic report generation. For more information about this portal, see the CounterACT Administration Guide.

To generate a report:

1. Select **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.



Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.

2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

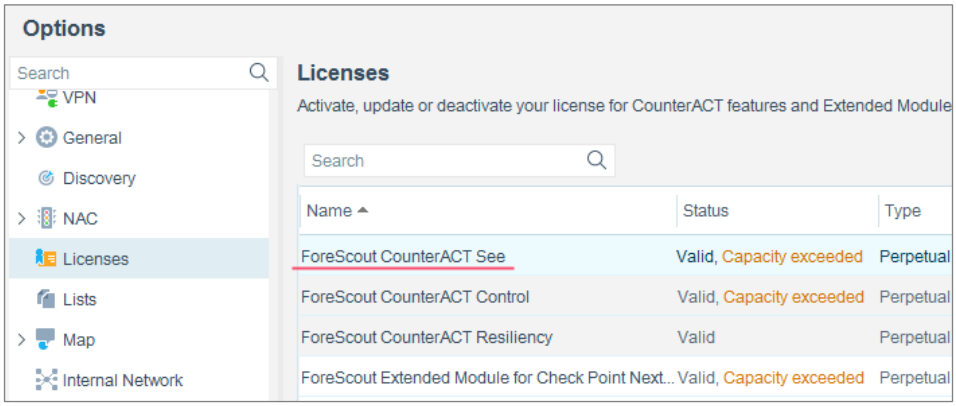
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-15 14:15