Table of Contents

About This How-to Guide ................................................................. 3
  Requirements .................................................................................. 3
  Supported Guest Management Portal Browsers ..................................... 3

About the Guest Management Portal .................................................. 3
  How the Portal Is Populated ............................................................. 4

What to Do ....................................................................................... 5

Configure Guest Registration Settings ............................................... 6
  Create Sponsors ............................................................................... 7
  How Sponsors Sign In to the Guest Management Portal ......................... 10
  Set Up a Password Policy .................................................................. 10
  Set Up Terms and Conditions .......................................................... 11
  Set Up Guest Notifications ................................................................ 13
    Guest Notifications ...................................................................... 15
  Set Up Sponsor Notifications .......................................................... 16
    Sample Email ............................................................................. 17
  Set Up Guest Tags ........................................................................... 18
  Purge Inactive Guests ...................................................................... 19

Manage Guests at the Console ............................................................ 20
  Add Guests ...................................................................................... 21
  Guest Management without Email Disclosure ...................................... 22
    Allow Guests to Self-Register without Email Disclosure ..................... 22
    Allow Sponsors to Add Guests without Email Disclosure .................... 25
  Require Registration Codes ................................................................ 26
  Remove Guests ............................................................................... 27

Set Up a Corporate/Guest Control Policy ........................................... 28
  Set Up a New Policy ........................................................................ 28
  Edit an Existing Policy .................................................................... 31
    Enable HTTP Login for Guests ....................................................... 32
    Enable Guest Registration ............................................................ 32
    Require Guest Verification ............................................................. 34

Edit/Localize Portal Messages and Labels ........................................... 38

Customize the Portal Appearance ....................................................... 38

Additional CounterACT Documentation ............................................ 40
  Documentation Downloads ............................................................. 40
  Documentation Portal ...................................................................... 41
  CounterACT Help Tools .................................................................. 41
About This How-to Guide

This guide provides information to CounterACT operators who control the guest management process. For information about what sponsors see at the portal and how to work with portal tools, refer to the Guest Management Portal for Sponsors How-to Guide. See Additional CounterACT Documentation for information on how to access the guide.

Requirements

This section describes the requirements for working with the Guest Management Portal.

- CounterACT version 8.0.
- Authentication Module version 1.0 or above with the CounterACT User Directory Plugin running.
- At least one Microsoft Active Directory server configured as an authentication server.
- A solid understanding of how to work with CounterACT policies and other CounterACT features, specifically the Guest Registration options, the HTTP Login action and the Corporate/Guest Control policy template.

Supported Guest Management Portal Browsers

The Guest Management Portal can be accessed using any of the following browsers:

- Internet Explorer 11x, Edge
- Safari 9.0 and above on MAC OS; Safari 8.3 and above on iOS
- Chrome 46 and above
- Firefox 43.0 and above
- Android Browser 1.5 and above

About the Guest Management Portal

The Guest Management Portal is a Web-based portal that enables corporate personnel to view and manage network guests who have requested access to the organization's network. When access is approved, guests can browse the network and possibly use other network resources.

Individuals who manage network guests from this portal are referred to as sponsors.

Sponsors can use the Guest Management Portal for various tasks, including:

- Viewing all their sponsored guests.
- Importing lists of guests to be granted network access, and adding a single guest. These guests are automatically approved for network access.
• Approving and declining guests who registered for network access using the Guest Registration form.
• Revoking network access to guests who were approved.
• Assigning and updating network access approval periods.
• Assigning tags to guests. Tags can be used in CounterACT policies.

The Guest Management Portal in your organization may look different from the examples shown in this document.

For information about what sponsors see at the portal and how to work with portal tools, refer to the Guest Management Portal for Sponsors How-to Guide. See Additional CounterACT Documentation for information on how to access the guide.

How the Portal Is Populated

The Guest Management Portal can be populated with guest information any of the following ways:

• By sponsors who use the Guest Management Portal to add guests to the network using the Add Guest page, and to import lists of guests using the import feature.
• By CounterACT operators who register guests from the CounterACT Console. See Manage Guests at the Console.
• By guests who register for network access using the Guest Registration form in a web browser. See Set Up a Corporate/Guest Control Policy.
What to Do

Perform the following to enable guest management in your organization:

1. Verify that your environment meets the requirements. See Requirements.

2. To enable the Guest Management Portal to be used for guest management, verify that the supported browsers are available to sponsors. See Supported Guest Management Portal Browsers.

3. In your User Directory Plugin, verify that at least one Microsoft Active Directory server is configured as an authentication server.
For more information about the plugin configuration refer to the CounterACT User Directory Plugin Configuration Guide. See Additional CounterACT Documentation for information on how to access the guide.

4. Configure the Guest Registration settings for your environment. See Configure Guest Registration Settings.

5. Set up a Corporate/Guest Control policy to handle unauthorized guest access to your network and to instruct CounterACT to work with Guest Management sponsors. See Set Up a Corporate/Guest Control Policy.

Configure Guest Registration Settings

CounterACT operators control the guest management process with a wide range of tools available at the Console. These include:

- Defining which corporate employees can be sponsors, or for which Active Directory group all members can be sponsors. See Create Sponsors. (Required for Guest Management Portal access)

- Defining the requirements for valid guest passwords (password policy). Guest management tools let you enforce your password policy when guests log in to your network. Password requirements are applied to both system-generated and guest-provided passwords. See Set Up a Password Policy.

- Customizing terms and conditions for guests and sponsors. These requirements reflect corporate policies and regulations. See Set Up Terms and Conditions.

- Defining which network access notification messages will be sent to guests. Notifications can be sent via email and text messages. See Set Up Guest Notifications.
- Defining which email confirmation notifications will be sent to sponsors. Emails contain guest contact information and login credentials for approved guests. See Set Up Sponsor Notifications.

- Defining tags that sponsors may be required to assign to guests in the Guest Management Portal. See Set Up Guest Tags.

- Purging inactive guests from the Guest Registration pane option in the Console and also from the Guest Management Portal. See Purge Inactive Guests.

- Adding pre-defined guests at the console. See Manage Guests at the Console.

### Create Sponsors

This section describes how to define corporate employees as sponsors. Only users defined as sponsors can log in to the Guest Management Portal to approve, decline or revoke network access for their sponsored guests.

- **All sponsor email addresses must be configured in Active Directory.**

Two types of sponsors can be created:

- **Sponsors** can view and manage only guests assigned to them.

- **Admin Sponsors** can view and manage all guests that have registered for network access, and can override the decisions of other sponsors.

Corporate employees whose contact emails are provided by guests in the Guest Registration form must be included in the Sponsors table, or they will not be able to access the Guest Management Portal.
Add Sponsors and Admin Sponsors in any of the following ways:

- Individually, by defining an email address
- As a group, by defining an Active Directory group
- Globally, by selecting all Active Directory members

To create sponsors:

1. In the CounterACT Console, select **Options** from the Tools menu. The Options pane opens.
2. Select **Guest Registration** and then select the Sponsors tab.
3. To define all your corporate Active Directory members as sponsors permitted to use the Guest Management Portal, select **All domain members are sponsors**. (Optional)

4. Select **Add**. The Add Sponsor dialog box opens.

5. Define the following:

<table>
<thead>
<tr>
<th><strong>Email\Active Directory Group</strong></th>
<th>Enter one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• the sponsor's Active Directory email address.</td>
</tr>
<tr>
<td></td>
<td>• an Active Directory group. This enables all group members to be sponsors.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th>Select a sponsor type.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Sponsors</strong> view and manage guests that are assigned to them.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Admin Sponsors</strong> are authorized to view and manage all guests and override the statuses applied by other sponsors.</td>
</tr>
</tbody>
</table>

| **Description** | Enter a description for the Guest Management sponsor entry. (Optional) |

6. Select **OK**.
How Sponsors Sign In to the Guest Management Portal

Sponsors sign in to the Guest Management Portal from their web browsers, and they authenticate using the same user name and password used when logging in to their corporate devices.

Ensure that sponsors are provided with the portal address so that they can access the Guest Management Portal.

**To sign in to the Guest Management Portal:**

1. Open a web browser and enter the organization's portal address in the address field. The portal address format is:
   
   ```
   https://X.X.X.X/sponsor
   ```
   
   where **X.X.X.X** is the IP address or the URL of the Enterprise Manager.

Set Up a Password Policy

Configure the validity requirements for guest passwords, such as the minimum length or special character requirements. The password policy is enforced when:

- guests define a password for logging in to your network
- CounterACT generates network passwords for guests

**To configure a password policy:**

1. Select **Options** from the Tools menu. The Options pane opens.
2. Select **Guest Registration** and then select the Password Policy tab.
3. Define any of the following password policy requirements:
   - Minimum length of a password
   - Minimum number of upper case letters
Guest Management for Operators

- Minimum number of lower case letters
- Minimum number of digits
- Minimum number of special characters. Valid special characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~

For information about using system-generated passwords and providing a Forgot my Password link, refer to the CounterACT Administration Guide, Define Guest Login Session Options section. See Additional CounterACT Documentation for information on how to access the guide.

Set Up Terms and Conditions

You can require guests and sponsors to agree to the use of your terms and conditions. Define the terms and conditions to present during guest management.

To configure terms and conditions:

1. Select Options from the Tools menu. The Options pane opens.
2. Select Guest Registration and then select the Terms and Conditions tab.
3. Define the following:

<table>
<thead>
<tr>
<th>Enable guest Terms &amp; Conditions</th>
<th>Require terms and conditions to be confirmed by guests prior to their registering or logging in.</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Define the URL displaying guest terms and conditions. Select Test to test the display of the terms and conditions in the URL.</td>
</tr>
</tbody>
</table>
### Text
Define a text of terms and conditions to present to guests. Select **Edit** to add, modify or delete terms and conditions.

### Enable sponsor Terms & Conditions
Require terms and conditions to be confirmed by sponsors prior to their approving guest network access.

### URL
Define the URL displaying sponsor terms and conditions. Select **Test** to test the display of the terms and conditions in the URL.

### Text
Define a text of terms and conditions to present to sponsors. Select **Edit** to add, modify or delete terms and conditions.

Guest terms and conditions must be accepted when the guest registers or logs in.

Sponsor terms and conditions are accepted automatically when the sponsor makes any changes at the Guest Management Portal.
Set Up Guest Notifications

You can instruct CounterACT when to send notifications to guests regarding their requests for access, and where to deliver these notifications. For example, instruct CounterACT to notify guests when they are approved or declined network access, and send the notification by SMS but not by email.

Email and phone information are provided:

- By sponsors when adding a guest in the Guest Management Portal
- In .csv files that are imported to the Guest Management Portal
By guests when they register for network access

By CounterACT operators who register guests from the CounterACT Console

To configure guest notification policies:

1. Select Options from the Tools menu. The Options pane opens.
2. Select Guest Registration and then select the Guest Notifications tab.
3. Select one or more in each category:

**Send notifications to guests via**

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Use email to deliver notifications to guests.</td>
</tr>
<tr>
<td>SMS</td>
<td>Use mobile text messaging (SMS) to deliver</td>
</tr>
<tr>
<td></td>
<td>notifications to guests.</td>
</tr>
</tbody>
</table>

**Send a notification upon account status changes**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Pending</td>
<td>Notify the guest that their network access request is pending.</td>
</tr>
<tr>
<td>Account Approval</td>
<td>Notify the guest that their network access request has been approved.</td>
</tr>
<tr>
<td>Account Rejection</td>
<td>Notify the guest that their network access request has been declined.</td>
</tr>
<tr>
<td>Account Revocation</td>
<td>Notify the guest that their network access approval has been revoked.</td>
</tr>
<tr>
<td>Account Expiration</td>
<td>Notify the guest that their network access approval period has expired.</td>
</tr>
</tbody>
</table>

**Guest Notifications**

This section provides an example of email notifications that guests may receive.

![Email Notification Example](image)

Sponsors can add messages to guests added through the Guest Management Portal.
You can change the default messages shown in emails and mobile text messages. See [Edit/Localize Portal Messages and Labels](#) for details.

**Set Up Sponsor Notifications**

You can instruct CounterACT when to send notifications to sponsors regarding the status updates they make at the portal. For example, instruct CounterACT to send confirmation emails to sponsors after they approve or decline network access.

- The sponsor can only approve or decline the guest if a Network Access Request email link is enabled. See [Sponsor approval using email link](#).

**To configure sponsor notifications:**

1. Select **Options** from the Tools menu. The Options pane opens.
2. Select **Guest Registration** and then select the Sponsor Notifications tab.
3. Define when to notify sponsors:

<table>
<thead>
<tr>
<th>Account</th>
<th>Notification Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Notify the sponsors when a guest has requested network access.</td>
</tr>
<tr>
<td>Approval</td>
<td>Notify the sponsors when they approve a guest’s network access request.</td>
</tr>
<tr>
<td>Rejection</td>
<td>Notify the sponsors when they decline a guest’s network access request.</td>
</tr>
<tr>
<td>Revocation</td>
<td>Notify the sponsors when they revoke a guest’s network access.</td>
</tr>
</tbody>
</table>

**Sample Email**

In the example below, an email is sent to a sponsor regarding a pending guest request. The email contains the guest request details.

You can update default messages shown in emails messages. See [Edit/Localize Portal Messages and Labels](#) for details.
Set Up Guest Tags

Use guest tags to categorize network guests into specific groups. For example, you can name your tags: AVP, Contractor, and Temp Worker. You can create policies that evaluate approved and declined guests based on their guest tag assignments. For example, create a policy that detects approved AVP guests and then assigns them to a specific VLAN or allows them maximum network access.

Sponsors can assign tags to guests through the Guest Management Portal.

After you create tags, you can configure CounterACT to require sponsors to assign one or several tags to guests, or allow sponsors to optionally assign tags.

To create tags:
1. Select Options from the Tools menu. The Options pane opens.
2. Select Guest Registration.
3. In the Registered Guests tab, select the Tags button. The Guest Tags dialog box opens.

4. You can select the following guest tag options:
   - **Sponsor may select multiple tags**: The sponsor can assign more than one guest tag.
   - **Sponsor is required to tag the guest**: The sponsor must assign a guest tag.

5. To add a new tag, select Add. The Add Guest Tag dialog box opens.
6. Enter the tag name.

7. If you select **Selected by default at the sponsor's page**, the tag is displayed when the Add Guest page is opened in the Guest Management Portal. The sponsor can manually remove it.

8. Select **OK**.

9. After all tags have been added, select **OK** to save the created guest tags in the CounterACT configuration.

10. Select **Apply** from the Guest Registration pane to ensure that Tags appear in the Guest Management Portal.

### Purge Inactive Guests

Guests become inactive when their status is changed to Declined, Revoked or Expired. Guests can be automatically purged a certain number of days after they become inactive. Inactive guest accounts are purged from the Guest Registration pane option in the Console and also from the Guest Management Portal.

**To purge inactive guests:**

1. Select **Options** from the Tools menu. The Options pane opens.
2. Select **Guest Registration**.
3. At the bottom of the Registered Guests tab, select **Purge after**.
4. Enter the number of days to wait before a guest is purged after its status is set to Declined, Revoked or Expired.

5. Select Apply.

Manage Guests at the Console

Guests can be managed from the Guest Registration pane option in the Console and also from the Guest Management Portal.

- **Operators** use the Registered Guests tab in the Guest Registration option of the Console and also the Guest Management Portal to view and manage all guests.
- **Sponsors** use the Guest Management Portal to view and manage only guests assigned to them.
- **Admin Sponsors** use the Guest Management Portal to view and manage all guests that have registered for network access, and to override the decisions of other sponsors.

<table>
<thead>
<tr>
<th>Task</th>
<th>Sponsors</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>View guests.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add pre-approved guests, including the following information:</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>- Full name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Email (Required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Phone number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Comment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add the following guest information:</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Date range of network access approval (Required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Tags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Message to be sent to the guest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Company name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Comment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add the following guest information:</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Password for network access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Tags.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Define global settings for:</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- password policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- HTTP Login actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- user and sponsor notifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve network access for guests who submitted a Guest Registration form.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Decline network access for guests who submitted a Guest Registration form.</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Add Guests

To add guests, operators can log in to:

- the Guest Management Portal as a sponsor and add the guests' identity information
- the Console and add the identity information and login credentials for the guests

It is recommended to add guests using the Guest Management Portal.

To add guests at the Console:

1. Select Options from the Tools menu. The Options pane opens.
2. Select Guest Registration. The list of guests is displayed.
3. In the Registered Guests tab, select Add. The Add Guest dialog box opens.
4. Complete the guest information, and provide a password for guest login.

   The **Restrict To** field is not used in this version.

5. Select **OK**.

6. After all guests have been added, select **Apply**. The added guests are automatically approved for network access.

7. It is the responsibility of your organization to forward the login credentials to the guests that were added at the Console. CounterACT does not do this for you.

The Registered Guests tab also supports:

- Importing guest entries into the tab from a CSV file. To initiate this action, select **Import**.
- Exporting guest entries from the tab into a CSV file. To initiate this action, select **Export**.

**Guest Management without Email Disclosure**

CounterACT identifies each guest by their Email field value.

**Allow Guests to Self-Register without Email Disclosure**

By default, guests registering for network access are required to enter a valid email address into the guest identification field of the Guest Registration form. If your organization does not want to require guests to share their email addresses, you can instruct CounterACT to allow guests to enter other identification information.

**To allow guests to self-register for network access without entering a valid email address:**

1. Use the Corporate/Guest Control policy wizard to create a policy for the appropriate scope.
2. In the policy wizard Guests tab, ensure that the **Show a Login page link where guests can register for full network access as Signed-in Guests** checkbox is selected.

3. In the Sub-Rules tab, double-click the **Guest Hosts** sub-rule to open it for editing.
4. In the Actions area, select the **HTTP Login** checkbox, and select **Edit**.
5. In the HTTP Login action, Registration Page tab, do the following:
   - Select the **Disable email validation** checkbox.
     This allows any string to be entered into the guest identification field of the Guest Registration form, even if it is not a valid email address.
   - Set the **Full Name** dropdown menu to **Hide**.
     This ensures that only one guest identification field is displayed in the Guest Registration form.

To change the strings of the guest identification fields that the user must enter on the Guest Registration form from *Email* to a different string:

1. Select **Options** from the Console **Tools** menu, and navigate to **Advanced > Language Localization > Endpoint Messages**.
2. In the Captive Portal actions, change the **Displayed** values of the following strings so that they reflect the type of guest identification required.

<table>
<thead>
<tr>
<th>Displayed</th>
<th>Type</th>
<th>Beginning of Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Label text</td>
<td>Captive Portal - Field label for: Email</td>
</tr>
<tr>
<td>Email Address; this will be your User Name when logging in to our network</td>
<td>Label text</td>
<td>Captive Portal - Field label for: Email (Guest Registration)</td>
</tr>
<tr>
<td>Enter your email address</td>
<td>Label text</td>
<td>Captive Portal - Field validation message for: 'Email' when is required</td>
</tr>
<tr>
<td>Enter your User Name (If you are a guest, enter your email address)</td>
<td>Label text</td>
<td>Captive Portal - Field validation message for: 'Username' when is required</td>
</tr>
<tr>
<td>Your User Name is your email address</td>
<td>Label text</td>
<td>Captive Portal - HTTP Login approve message</td>
</tr>
</tbody>
</table>

3. You can change the guest identification label displayed to operators in the HTTP Login action so that it reflects the type of guest identification required. In the HTTP Login actions, change the **Displayed** values of the following string:

<table>
<thead>
<tr>
<th>Displayed</th>
<th>Type</th>
<th>Beginning of Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Label text</td>
<td>Guest Registration Email form field label</td>
</tr>
</tbody>
</table>

**Allow Sponsors to Add Guests without Email Disclosure**

By default, sponsors are required to enter a valid email address into the guest identification field of the Guest Management Portal. You can instruct CounterACT to allow sponsors to add guests using other identification information.

**To allow sponsors to add guests without valid email addresses:**

1. Select **Options** from the Console **Tools** menu, and navigate to **Guest Registration**.
2. In the User Policy tab, select **Disable Email Validation**.
To change the strings of the guest identification fields that the sponsor must enter in the Guest Management Portal from Email to a different string:

1. Select Options from the Console Tools menu, and navigate to Advanced > Language Localization > Endpoint Messages.

2. In the Guest Management Portal actions, change the Displayed values of the following strings so that they reflect the type of guest identification required.

<table>
<thead>
<tr>
<th>Displayed</th>
<th>Type</th>
<th>Beginning of Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each guest must have a unique email. {0} appears in lines {1}.</td>
<td>Error text</td>
<td>Error message for when guest list contains 2 or more guests with same...</td>
</tr>
<tr>
<td>Email</td>
<td>Label text</td>
<td>The Email label that appears in the Add Guest form</td>
</tr>
<tr>
<td>Email</td>
<td>Label text</td>
<td>The Email header that appears in the Guest Management Portal...</td>
</tr>
<tr>
<td>Email</td>
<td>Label text</td>
<td>Import Guests instructions text: step 2 Email column</td>
</tr>
<tr>
<td>Email address</td>
<td>Label text</td>
<td>Text that appears in New Guest page, Email field</td>
</tr>
<tr>
<td>Email address '{0}' has been added to the portal.</td>
<td>Label text</td>
<td>Approved success message</td>
</tr>
<tr>
<td>Enter an email address.</td>
<td>Error text</td>
<td>Empty email address is not allowed</td>
</tr>
<tr>
<td>Enter an email address.</td>
<td>Label text</td>
<td>Error displayed to user in New Guest page when the user did not enter...</td>
</tr>
<tr>
<td>The email address is too long. Enter up to 48 characters.</td>
<td>Label text</td>
<td>Guest form validation error when user entered an email with too much...</td>
</tr>
<tr>
<td>The guest at email address '{0}' has been updated.</td>
<td>Label text</td>
<td>Update success message</td>
</tr>
<tr>
<td>The portal already contains an Approved or Pending guest with email address...</td>
<td>Error text</td>
<td>Email address already exists. Can't override guest with status Approved...</td>
</tr>
</tbody>
</table>

**Require Registration Codes**

Registration codes are used when working with the HTTP Login action that requires guests to register before the Guest Registration request is processed. If the guest does not provide the correct code, the request is not processed. Use this feature to ensure that only guests with whom you've shared the registration code can apply for network access.

To use this feature, enable the Require Registration Code option in the HTTP Login action, Registration Page tab.

To retrieve registration codes to send to guests:

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

3. In the Registered Guests tab, select **Codes**. The Registration Codes dialog box opens and displays the daily registration codes.

4. A unique code is shown for each day. Identify the registration code for the day you expect your guest to require network access.

5. It is the responsibility of your organization to forward the code to the network guests. CounterACT does not do this for you.

**Remove Guests**

Guests that you remove are automatically and immediately signed out of the network, and their accounts are purged from the Guest Registration pane option in the Console and also from the Guest Management Portal. Users who are removed while still browsing are notified by a web message of this management action.

**To remove a guest:**

1. In the Registered Guests tab of the Guest Registration pane, select a guest entry.

2. Select **Remove** and then select **Apply**.
In the Guest Management Portal, sponsors can revoke their approved guests and decline guest requests, but they cannot remove guests from the system. Revoked and declined guests are eventually removed by the Purge Inactive Guests feature.

Set Up a Corporate/Guest Control Policy

Endpoints that do not meet the criteria as Corporate Hosts or Signed-in Guests are classified as Guest Hosts, and users at these endpoints are called guests. These may include, for example, visiting professionals, contractors or university students, or corporate members using personal devices that are not currently known to CounterACT.

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.

You should have a solid understanding of how the Corporate/Guest Control policy works.

Set Up a New Policy

Use the Policy Wizard to create a Corporate/Guest Control policy.

In the Guests page of the policy wizard, select or clear the following options:

- **Show a Login page link where guests can register for full network access as Signed-in Guests**: This option allows guests to use a Guest Registration form in a web browser to request network access. If this option is not selected, guests can only be added to the Guest Management Portal by sponsors or by CounterACT operators using the Console.

- **Guests must be approved by the sponsor they provide, or by**: Select this option to require sponsor approval before guests can access the network. Email addresses must be comma-separated. If the Sponsor Notifications, Account Pending setting is selected, the guest registration information is sent for sponsor approval to the contact specified by the guest and also to the email addresses in this window.

- **To allow limited network access to unapproved guests, select Allow guests to skip login and have limited access only**.
The following are examples of ways to handle unauthorized users:

- **Network access requests are automatically approved**
  Allow users to enter identity information on a Guest Registration form in a web browser and then receive login credentials. To use this option, select **Show a Login page link where guests can register for full network access as Signed-in Guests**, and clear **Allow guests to skip login and have limited access only**.

- **Pre-approve guests using the Guest Management Portal**
  Users designated as corporate sponsors in the Console Guest Registration settings can add guests to the Guest Management Portal. These guests are automatically approved, and login credentials are emailed to them. To use this option, select **Guests must be approved by the sponsor...**, and clear **Allow guests to skip login and have limited access only**.

- **Pre-approve guests in the Console**
  Operators can define identity information and login credentials for guests at the Console. When these guests log in to your network, the credentials they submit are checked against the credentials that the operator defined. It is the responsibility of your organization to forward the credentials to the guests. CounterACT does not do this for you. To use this option, clear **Allow guests to skip login and have limited access only**.

- **Let guests skip the both the registration and the login process**
  All unauthenticated users are able to enter the network with limited access. There are no login requirements for limited access. To use this option, select **Allow guests to skip login and have limited access only**.

- **Let users sign in with credentials, without registration**
Force users to sign in with valid credentials, with no option to register as a guest. Until they sign in, users at these endpoints will not be able to enter the network at all. To use this option, clear **Show a Login page link where guests can register for full network access as Signed-in Guests**, and clear **Allow guests to skip login and have limited access only**.

- **Let users enter the network with limited access**

  Allow unauthorized users to either register to receive login credentials, or skip login and enter the network with limited network access. To use this option, select **Show a Login page link where guests can register for full network access as Signed-in Guests** and select **Let unauthorized users skip Sign In**.

To set more options, you can edit the *Guest Hosts* sub-rule. See [Edit an Existing Policy](#).

**Activating the Registration Process**

By default, the HTTP Login policy action used to activate the Guest Registration form and other web pages or emails used for the guest registration process is disabled. This means that if you choose to enable guest registration from the policy template, you still must activate the registration process from the policy sub-rule.

The policy template is designed this way so that you can run the policy once to get a sense of how your endpoints are classified, fine-tune the policy, and then activate the corporate login and guest registration process.

**To activate this process:**

1. Right-click the *Guest Hosts* sub-rule for this policy from the Policy Manager.
2. Select *Quick Edit* and then select *Actions*.
3. In the Action dialog box, enable the **HTTP Login** action.
4. Select **OK**.

5. In the Policy Manager, select **Apply**.

The login and guest registration actions are activated. During login, guests are presented with a Guest Registration form to complete.

---

**Edit an Existing Policy**

In a Corporate/Guest Control policy, open the *Guest Hosts* sub-rule for editing, and edit the HTTP Login action, Guests tab.
Enable HTTP Login for Guests

Ensure that **Enable HTTP login for approved guests** is selected so that approved guests can access the network. You can select or clear any other options.

To use the **Keep open a 'Login Session' window after guest login** feature, the pop-up blocker must be disabled on the guest’s browser or the popup must be approved manually.

Enable Guest Registration

Select **Show a Login page link where guests can register for full network access as Signed-in Guests** to allow guests to use a Guest Registration form in a web browser to request network access. These guests are added to the Guest Management Portal as **Pending** guests. If the **Sponsor Notifications**, Account Pending setting is selected, the guest registration information is sent for sponsor approval to the contacts specified by the guest and to the **Pre-defined sponsors** defined in this window.

If this option is not selected, guests can only be added to the Guest Management Portal by sponsors or by CounterACT operators using the Console.

The following settings apply only when a guest requests network access using a Guest Registration form.
- **Provide a system-generated password to self-registering guests:**
  Instructs CounterACT to hide the Password fields in the Guest Registration form, and to generate network passwords for guests upon sponsor approval. If this option is not selected, guests select their own passwords in the Guest Registration form. Both system-generated and guest-provided passwords must meet the configured password policy requirements. See Set Up a Password Policy.

- **Guests added by sponsors using the Guest Management Portal are always sent system-generated passwords.**
  The passwords of guests added using the Console are always set by the CounterACT operator.

- **Limit guest accounts to:** Defines the maximum network access period allowed for self-registering guests. By default, this field is unselected, making the maximum network access approval period **unlimited**. In the Guest Management Portal, sponsors can further limit the network access of their self-registering guests to less than this value.

- **Guests must be approved by the sponsor...:** Requires sponsor approval before the guest can access the network. The guest remains in Pending status until approved by a sponsor.

- **Only sponsors included in the Guest Registration, Sponsors list can use the Guest Management Portal.** See Create Sponsors.

- **Enable sponsor approval without authentication via emailed link:**
  Provides sponsors with a basic Approve/Decline Network Access Request web page accessed by an email link. Sponsors can approve or decline guests, and also include messages in the guest's Approval or Declined notification, using either this web page or the Guest Management Portal.

- **If Enable sponsor approval without authentication via emailed link is selected, it is recommended to select Sponsors must be in these domains to ensure that only corporate employees receive the emailed link.** See Create Sponsors.
- **Pre-defined sponsors for all guests**: contains the sponsor email addresses defined when the policy was created. If Sponsor Notifications settings are selected, email addresses in this field, together with the contact emails entered by the guest in the Guest Registration form, receive email notifications about the guest. Sponsor emails added in this window can only manage those guest requests added after this configuration change is applied.

## Require Guest Verification

Verification codes are used when working with the HTTP Login action that requires guests to register before the Guest Registration request is processed. Use this feature to verify that the email address or phone number entered by the guest in the registration form is valid. CounterACT sends a one-time verification code to the guest email address or mobile phone number that they entered in their registration form, and then requires the guest to enter the code before logging in.

![Submit Verification Code](image)

Verification codes are automatically generated and validated by CounterACT. Enable the registration code option from the Guests tab in the HTTP Login action.

**To work with verification codes:**

1. In the HTTP Login action, select **Require Verification Code** in the Guests tab.

2. From the drop-down list, select whether the verification code will be sent via email only, via mobile phone only, or via both email and mobile phone.
A customized message is included in the email. The mobile text message includes only the verification code.

**Define Mobile Carrier**

To send a verification code to a mobile device, you must define how CounterACT submits the message to the mobile carrier.

To define text messaging through a mobile carrier:

1. Select **Options** from the **Tools** menu and then select **General > Mobile Text Message**.
2. Select **Add**. The Carrier Type dialog box opens.

![Carrier Type dialog box](image)

Select **Mail Carrier** to send text message requests to a carrier in email format, or select **URL Carrier** to send text message requests to a carrier in a URL string.

3. Select **OK**. In the Add Carrier dialog box, enter a name that identifies this carrier in the **Name** field. In the other fields of the dialog box, enter string patterns that define the format used to submit message requests.

   - For message requests in email format, the fields correspond to the Address, Subject, and Message fields of an email message.
For message requests in URL format, a single URL field is used to submit the message request. In addition, an optional Proxy URL field lets you specify an alternative URL.

In these fields, use the following parameters as placeholders for values that are inserted into the request:

- `_PHONE_NUMBER_` is the target phone number for the text message. For example, for guest registration this is the phone number submitted by the guest.
- `_MESSAGE_` is message text inserted in the request. For example, for guest registration this is the registration code.

4. Select **Test** to send a sample message request using the defined format. Enter values for the `_PHONE_NUMBER_` and `_MESSAGE_` parameters, and select **OK** to submit the message request. Confirm receipt of the test message on the target mobile device.

5. In the Add Carrier dialog box, select **OK**. The carrier is added to the list in the Mobile Text Message pane.
Edit/Localize Portal Messages and Labels

You can edit or localize text that appears in the Guest Management Portal, including error messages, email messages and labels.

To edit or localize text:

1. Select Options from the Tools menu. The Options pane opens.
3. Type Guest Management Portal in the search field to view all the Portal texts that can be edited. The currently displayed texts are in the Displayed column.
4. Select the row with the text you want to change, and select Edit.
5. Enter the new text, and select OK.
6. When you are done editing the texts, select Apply.

Customize the Portal Appearance

You can customize the appearance of the Guest Management Portal with the look-and-feel and branding requirements of your organization.

Before customization:
Example of customization:

To customize the portal, the operator must have SSH access to the Enterprise Manager or the standalone CounterACT Appliance.

For information about customizing the Guest Management Portal user interface, refer to the *CounterACT Administration Guide, The CounterACT User Portal Builder* section. See [Additional CounterACT Documentation](#) for information on how to access the guide.
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:**

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:**

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:**

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 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-15 14:22