Forescout

Guest and Corporate Management

How-to Guide for Operators

Forescout version 8.2
Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2020 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.
# Table of Contents

**About the User Directory Plugin** .............................................................. 5  
**What to Do** .......................................................................................... 5  
**Corporate/Guest Control Policy** ............................................................. 5  
  Groups Populated by a Corporate/Guest Control Policy ......................... 6  
  Corporate Hosts .................................................................................... 6  
  Signed-In Guests ................................................................................. 6  
  Guest Hosts ....................................................................................... 7  
**Using the Corporate/Guest Control Policy Template** ............................. 7  
  Which Devices Are Inspected – Policy Scope .......................................... 8  
  Handling Guest Hosts – Guests Page ..................................................... 9  
**Saving the Policy** ................................................................................ 11  
**Fine-Tuning the Policy** ........................................................................ 11  
**Enabling the Guest Hosts Sub-Rule Actions** ......................................... 11  
**What to Do When Authentication Server Values Are Changed** .............. 13  
**Report Generation** ............................................................................... 13  
**Guest Management from Portal and Console** ......................................... 14  
  How Guests Are Added ........................................................................... 14  
  How Guests Are Managed ...................................................................... 15  
**Guest Management Portal** .................................................................... 16  
  Guest Management Pane ....................................................................... 17  
**Support for Guest Management without Email Disclosure** .................. 33  
  Allowing Guests to Self-Register without Email Disclosure ..................... 33  
  Allowing Sponsors to Add Guests without Email Disclosure .................... 37  
**HTTP Login Action Configuration** ......................................................... 38  
  Handling Guests .................................................................................... 40  
  Handling Corporate Users ...................................................................... 41  
**HTTP Login Action Tabs** ...................................................................... 41  
  Login Page Tab .................................................................................... 41  
  Guests Tab .......................................................................................... 43  
  Corporate Tab .................................................................................... 54  
  Registration Page Tab .......................................................................... 56  
  Miscellaneous Tab ............................................................................. 59  
**Customize HTTP Login Action Text** ....................................................... 60  
**Track Repeated Login Failures** ............................................................... 60  
**Endpoint Redirection** .......................................................................... 61  
  Hijack Methods .................................................................................... 61  
  Centralized Web Authentication Method ................................................. 61  
  Packet Engine Method .......................................................................... 62  
  DNS Enforce Plugin Method ................................................................... 62  
**Advanced Redirection Configuration** ...................................................... 62
Guest Management Interface Customization................................................. 63
  Localize Web Pages and Messages............................................................63
  The Forescout User Portal Builder..............................................................64
    Opening the User Portal Builder.............................................................65
    Using the User Portal Builder to Customize Skins....................................66
    Deploying a Skin for a User Interface....................................................69

Additional Forescout Documentation.......................................................... 69
  Documentation Downloads ......................................................................69
  Documentation Portal ..........................................................................70
  Forescout Help Tools.............................................................................70
About the User Directory Plugin

The User Directory Plugin is a component of the Forescout Authentication Module. The plugin is comprised of two components.

- User Directory server configurations
- Guest and Corporate Registration configuration

The plugin resolves endpoint user details and performs user authentication via configured internal and external directory servers. For information about server configurations, refer to the User Directory Plugin guide.

What to Do

Perform the following to configure Forescout corporate and guest management:

1. Ensure that your network meets the system requirements, and configure the User Directory Plugin. Verify that at least one Microsoft Active Directory server is configured as an authentication server. For more information, refer to the Forescout User Directory Plugin Configuration Guide. See Additional Forescout Documentation for information on how to access this guide.

2. Set up a Corporate/Guest Control policy to handle unauthorized guest access of your network and instruct the Forescout platform to work with Guest Management sponsors. See Corporate/Guest Control Policy.

3. Optionally run a report to see real-time information about corporate and guest hosts. See Report Generation.

4. Configure guest registration and management options. See Guest Management from Portal and Console and HTTP Login Action Configuration.

Optionally personalize your corporate Guest Management Portal, web messages and labels. See Guest Management Interface Customization.

Corporate/Guest Control Policy

To control access to your corporate network, Forescout platform provides tools that let you find and classify hosts in your network. Use the Corporate/Guest Control policy template to create a policy that:

- Organizes endpoints into Guest Hosts, Signed-In Guests and Guest Hosts groups.
- Enforces network restrictions on users at unauthorized endpoints.
- Allows users at unauthorized endpoints to request network access as guests.

The list of corporate guests is stored in the Forescout Console.

By default, the Corporate/Guest Control policy template is designed to prompt users using non-corporate hosts to register (request access) as network guests by entering their contact details in a Guest 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.

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

This section covers:
- Groups Populated by a Corporate/Guest Control Policy
- Using the Corporate/Guest Control Policy Template
- What to Do When Authentication Server Values Are Changed

**Groups Populated by a Corporate/Guest Control Policy**

**Corporate Hosts**
Corporate Hosts are endpoints that are currently signed in as a Domain User or have authenticated recently to an approved authentication server.

If at least one of the following criteria is met, the endpoint is added to the Corporate Hosts group. Hosts that do not meet any of these criteria are added to the Signed-in Guests group or the Guest Hosts group.

**The Endpoint Recently Authenticated to an Approved Authentication Server**
This criterion detects if the endpoint authenticated with an approved authentication server within the last four weeks.

Authentication servers can be defined during the initial setup, and in the Tools > Options > NAC > Authentication window.

For information about working with the Corporate/Guest Control policy after authentication server definitions change, see What to Do When Authentication Server Values Are Changed.

**The Endpoint Is Currently Signed In as a Domain User**
This criterion detects if the endpoint is signed in as a domain user.

**Signed-In Guests**
Hosts that were not categorized as Corporate Hosts are evaluated to see if they are Signed-in Guests.

This sub-rule detects if the endpoint meets one of the following criteria:
- the user is currently signed-in to your network as a Signed-in Guest
- the user successfully logged in as a Signed-in Guest via the HTTP Login action within the last 12 hours
- the user is approved based on their Guest Registration status
A *Signed-in Guest* is a user who was not authorized to enter the network as a corporate user but later received a valid user name and password. These credentials were successfully used in a Login page when the *Signed-in Guest* attempted to access the Internet.

**Guest Hosts**

Hosts that do not meet the criteria as *Signed-in Guests* are categorized as *Guest Hosts*.

**Using the Corporate/Guest Control Policy Template**

Deploy a policy created by the Corporate/Guest Control policy template to classify your network into Corporate Hosts, Signed-in Guests and Guest Hosts groups, and to deploy options for handling guests.

Before creating the policy:

- Consider which endpoints you want to inspect, specifically segments in which guests may connect to the network. The template does not handle endpoints outside of the Internal Network.
- Verify that your Primary Classification policy is applied to the network segment or IP address range on which you want to apply the Corporate/Guest Control policy.
- The Corporate/Guest Control policy does not apply to printers and network devices, which are detected and classified by the Primary Classification policy.

**To create the policy from the template:**

1. Select **Add** from the Policy Manager.
2. Select **Corporate/Guest Control**.
3. Select **Next**. The Name page opens.
4. Edit the name if required and add a description.
5. Select **Next**. The Scope page opens.

**Which Devices Are Inspected – Policy Scope**

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 pane.
- **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 page.
3. To filter the specified ranges or add exceptions, select (Advanced).

Handling Guest Hosts – Guests Page

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 the Forescout Console.

Use the options here to define how you want to handle guests. These options are disabled by default. The template is set up this way so that you can first review endpoint classification, perform fine-tuning, and then enable sub-rule actions to easily activate a registration process that meets your corporate needs.

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. If the checkbox is cleared, guest registration must be initiated by a sponsor in the Guest Management Portal or by a Forescout Console operator in the Guest Registration Pane.

Select Guests must be approved by the sponsor... to share the registration information submitted by the guest with designated corporate contacts, called sponsors, who can be designated by the guest. A sponsor must approve the guest before the guest is granted network access.
Sponsor email addresses must be included in the Guest Registration, Sponsors tab. For more information about sponsors, see Create Sponsors.

The following are examples of ways to handle unauthorized users:

- **Require guests to submit their contact information before being 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 Network access requests are automatically approved, and clear Allow guests to skip login and have limited access only. See HTTP Login for details.

- **Require guests to be approved by a sponsor**

  Users designated as sponsors can approve guests in the Guest Management Portal, and Forescout platform sends network access credentials to these guests. To use this option, select Guests must be approved by the sponsor..., and clear Allow guests to skip login and have limited access only.

- **Allow network access to pre-approved guests only**

  - Sponsors can add pre-approved guests to the Guest Management Portal. Forescout platform generates and sends login credentials to these guests.
  
  - Operators can define identity information and login credentials for pre-approved guests at the Console. It is the responsibility of your organization to forward the credentials to the guests.

  No other guests are authorized to log in to your network. 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. See Adding Guests for information about manually adding guests.

- **Always allow guests limited access only**

  There are no login requirements for limited access, and all unauthenticated users can enter the network with limited access only. Unauthorized guests cannot request full network access. To use this option, clear Show a Login page link where guests can register for full network access as Signed-in Guests, and select Allow guests to skip login and have limited access only.

- **Let users enter the network with limited access or request full 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 Allow guests to skip login and have limited access only.
Saving the Policy

- Select Next and then select Finish to save the new policy.

Fine-Tuning the Policy
The Corporate/Guest Control policy template is designed so that the Add to Group actions are the only actions enabled. Endpoints are automatically classified into Corporate Hosts, Signed-in Guests, and Guest Hosts groups.

1. To review each group generated by the policy, select the group in the Filters pane in the Console, under the Groups node. The associated endpoints are displayed in the Console's Detections pane.

2. If the groups do not accurately reflect your corporate needs, return to the Policy Manager, select the Corporate/Guest Control policy you created, and modify the rules.

Enabling the Guest Hosts Sub-Rule Actions
By default, the HTTP Login, Assign to VLAN and Virtual Firewall policy actions are disabled in the Guest Hosts sub-rule. After ensuring that your endpoints are classified according to your corporate needs, you can enable the policy's sub-rule actions for guest registration or guest access restrictions.

To enable the disabled policy actions:

1. In the Policy Manager, right-click the Guest Hosts sub-rule for your Corporate/Guest Control policy.

2. Select Quick Edit.

3. Select Actions and enable the actions you want to apply to unauthorized guests:
   - HTTP Login
   - Assign to VLAN
   - Virtual Firewall

4. Select OK and then Apply.

HTTP Login
The HTTP Login action is used to activate the Guest Registration form and other web pages and emails used for the guest registration process. The action prompts unauthorized users to either sign in or complete a Guest Registration form with identity information. This provides you with registration information for each guest, such as contact details and the name of the individual who invited the guest to the network. All users attempting to access the corporate network are presented with a Login page where they can choose how to proceed. The Login page remains until login succeeds or is skipped, or if the endpoint is released via the Console or the Assets Portal.
Login Page and Guest Registration Form

You can configure the HTTP Login action to handle unauthorized users in the following ways:

**Automatically approve guest registrations**

For guests to be automatically approved after completing the Guest Registration form, select *Network access requests are automatically approved* in the Guests page of the policy wizard. You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who registered. Guests fill out a Guest Registration form with identity information, including an email address field. Identity information is stored on a guest server (the Appliance) and can be viewed by a sponsor in the Guest Management Portal or by a Forescout operator in the Guest Registration Pane. See **Guest Management from Portal and Console**. Guests log in using the value in their email address field as their user name, together with a password that they defined during registration.

**Require email approval by an authorized corporate sponsor**

For guests to be approved by authorized individuals, called *sponsors*, in your organization, select *Guests must be approved by the sponsor...* field. In addition to the sponsor named by each guest, you can define additional pre-defined sponsors for guests by typing the email addresses of these sponsors in the field. Email addresses must be comma-separated. There is no limit to the number of sponsors that you can list, and only one must grant approval. After approval, guests are sent a password that is automatically generated by Forescout platform. When guests log in to the network, their credentials are checked against the credentials that were approved. Identity information is stored on a guest server (the Appliance) and can be viewed by a sponsor in the Guest Management Portal or by a Forescout operator in the Guest Registration Pane. See **Guest Management from Portal and Console**.

For more information about configuring the HTTP Login action, see **HTTP Login Action Configuration**.
**Assign to VLAN**

The *Assign to VLAN* action restricts guest access by moving guest hosts to a predefined VLAN from which network access can be restricted. A Guest VLAN must be included in the IP address range defined for this policy. The VLAN must be defined on all switches on which guest hosts can be found.

**Virtual Firewall**

The *Virtual Firewall* action blocks guests from your network.

**What to Do When Authentication Server Values Are Changed**

If authentication server values are changed after creating a policy from the template, the policy values must be updated manually. Specifically, parameters defined in the policy are not linked to the new authentication settings. You can update policy credentials via a property *List* – an editable list of these credentials that was automatically generated with the policy.

**Report Generation**

After the Corporate/Guest Control 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.

患有 The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the Forescout Console User 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.
Guest and Corporate Management from Portal and Console

Many organizations want to provide limited network and Internet access to company visitors, such as contractors, visiting professionals, and other network guests. The HTTP Login action can detect, register and control network guests. For more information about the HTTP Login action, see HTTP Login Action Configuration. Requests for guest access to your corporate network can be generated when the HTTP Login action is:

- Applied manually to detected endpoints
- Applied during a Forescout Corporate/Guest Control policy evaluation of detected endpoints

How Guests Are Added

Guest information is stored in a guest list which can be populated in any of the following ways:

- By guests who request network access using the Guest Registration form in a web browser. See Handling Guests.
By sponsors who add pre-approved guests or import lists of pre-approved guests at the Guest Management Portal.

By Forescout operators who add pre-approved guests in the Guest Management Portal.

**How Guests Are Managed**

Guests can be managed in any of the following ways:

- Forescout operators can use the Registered Guests tab in the Guest Management Pane to view and manage all guests and to configure guest management features.
- Sponsors can use the Guest Management Portal to view and manage 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>Guest Management Task</th>
<th>Sponsors Using Guest Management Portal</th>
<th>Operators Using Guest Registration Pane</th>
</tr>
</thead>
<tbody>
<tr>
<td>View guests.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add pre-approved guests, and include 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>Guest Management Task</td>
<td>Sponsors Using Guest Management Portal</td>
<td>Operators Using Guest Registration Pane</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Include the following additional guest information when adding or approving guests:</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>Include the following additional guest information when adding or approving guests:</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>▪ Password for network access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create tags to be assigned to guests.</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>
<tr>
<td>Revoke guests who were approved for network access.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remove guests from the Console and the Guest Management Portal guest lists.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Automatically purge guests a certain number of days after their accounts expired, were declined, or were revoked. Purging removes them from the Console and the Guest Management Portal guest lists.</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**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 Forescout policies.

Sponsors' corporate email addresses must be included in the Sponsors table, so that they can access the Guest Management Portal. See Create Sponsors.

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

For detailed information about working with the Guest Management Portal, refer to the following document.

- Guest Management Portal for Sponsors How-to Guide

See Additional Forescout Documentation for information on how to access these guides.

You can localize the strings in the Guest Management Portal. See Localize Web Pages and Messages.

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

**Guest Management Pane**

In the Guest Management, Registered Guests tab, Forescout operators can perform the following guest management activities.

- Add approved guests, edit and remove them:
  - Adding Guests
  - Removing Guests
  - Purging Inactive Guests
  - Editing Guests
Guest and Corporate Management How-to Guide for Operators

- Generate registration codes. See Retrieving Registration Codes.
- Define tags that sponsors can assign to guests at the portal. See Managing Guest Tags.
- Define a password policy that will be enforced when passwords are system-generated or self-selected by guests for login to the corporate network. See Define a Password Policy.
- Define how certain guest fields are validated. See Define a User Policy.
- Define the corporate sponsors who can use the Guest Management Portal for managing guests. See Create Sponsors.
- Define terms and conditions that reflect your corporate policies and regulations, and require their acceptance by guests accessing your network and by sponsors using the Guest Management Portal. See Define Terms and Conditions.
- Define the way Forescout platform notifies guests about their network access status, and sends their login credentials. Notifications can be sent via email and text messages. See Guest Notifications.
- Define which notifications are emailed to corporate sponsors about their guests' network access status. See Sponsor Notifications.

When you are finished configuring the Guest Management pane, select Apply to save your changes in the Forescout configuration.

The Forescout user who works with Guest Registration functionality must have the Plugin Management update permission.

**Guest Management Pane**

To open the Guest Management pane:

- Select Options from the Console Tools menu and then select Guest Management. The Guest Management pane opens.
Adding Guests

If you know ahead of time that your organization is expecting guests and you have their identity information, you can pre-approve the guests and later verify that they are authenticated.

- **Individuals defined as Sponsors can add and import pre-approved guests directly to the Guest Management Portal. It is recommended to add guests using the Guest Management Portal. Refer to the Guest Management Portal for Sponsors How-to Guide. See Additional Forescout Documentation for information on how to access this guide.**

**To view and add guests at the Console:**

1. Select the Registered Guests tab of the Guest Management pane. The list of guests is displayed.

![Registered Guests](image)

2. To add a guest, select **Add**. The Add Guest dialog box opens.

![Add Guest](image)

3. Complete the guest information, and provide a password for guest login.
   - **The Restrict To field is not used in this version.**

4. Select **OK**.
5. After all guests have been added, select **Apply**. The added guests are automatically approved for network access.

6. It is the responsibility of your organization to forward the login credentials to guests added at the Console. Forescout platform 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**.

**Removing Guests**

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

> In the Guest Management Portal, sponsors can revoke their approved guests and decline guest requests. Refer to the Guest Management Portal for Sponsors How-to Guide. See Additional Forescout Documentation for information on how to access this guide.

**To remove a guest:**

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

2. Select **Remove** and then select **Apply**.

**Purging 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 both the Forescout Console and the Guest Management Portal.

**To purge inactive guests:**

1. At the bottom of the Registered Guests tab of the Guest Management pane, select **Purge after**.
2. Each guest is purged from the guest list a certain number of days after its status is set to Declined, Revoked or Expired. Enter a value for the number of days to wait before purging these guests.

3. Select Apply.

**Editing Guests**

You can edit guest registration values. If you update the password, you must notify the guest.

**To edit a guest:**

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

2. Select Edit. The Edit Guest dialog box opens.

3. Update the guest information.

4. Select OK and then select Apply.

In the Guest Management Portal, sponsors can edit the approval period requested by guests. Refer to the Guest Management Portal for Sponsors How-to Guide. See Additional Forescout Documentation for information on how to access this guide.

**Retrieving Registration Codes**

Registration codes can be used when the HTTP Login action 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.

Enable the registration code option from the Registration Page tab in the HTTP Login action.
To retrieve registration codes to send to guests:

1. In the Registered Guests tab of the Guest Management pane, select **Codes**. The Registration Codes dialog box opens and displays the daily registration codes.

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

3. It is the responsibility of your organization to forward the code to the network guests. Forescout platform does not do this for you.

**Managing Guest Tags**

The Forescout operator creates guest tags in the Guest Management pane. Sponsors can assign these tags to guests:

- when approving or declining guests using the Network Access Request page opened by the emailed link
- when adding guests in the Guest Management Portal

Guest tag assignment is not available to sponsors when approving pending guests in the Guest Management Portal.
To use the Tags feature, **Guests must be approved by the sponsor**... must be selected in the Guests tab of the HTTP Login action.

You can create policies that evaluate guests for specific guest tag assignments. For example, create a policy that detects guests tagged as VIP guests and assigns them to a specific VLAN or allows them maximum network access.

To work with tags, perform the following:

- Configure Tags
- Create Policies with Your Tags

**Configure Tags**

Create tags that sponsors can assign to guests.

**To configure tags:**

1. In the Registered Guests tab of the Guest Management pane, select Tags.

2. In the Guest Tags dialog box, you can select guest tag options:
- **Sponsor may select multiple tags**: Enables the sponsor to assign multiple tags to each guest.
- **Sponsor is required to tag the guest**: Requires the sponsor to assign at least one tag to each guest.

If you do not select any option, sponsors can optionally assign each guest a single tag.


4. Enter a name for the new tag.

5. If you select **Selected by default at the Guest Management Portal**, the tag appears by default in the Add Guest page in the Guest Management Portal. The sponsor can manually remove it from the Add Guest page.

6. Select OK.

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

*Create Policies with Your Tags*

Control guests based on their guest tags. Do this by incorporating the evaluation of the Guest Tags property in your policies.

For example, create a policy that detects guests with an Authentication, Signed In Status property value of Signed In as a Guest and a Guest Tag property value of Building A and then assigns them to a specific VLAN or allows them minimum network access.

*To incorporate guest tags:*

1. Edit or create a policy.

2. Define the condition so it includes the Guest Registration > Guest Tags property. The list of available property values contains all the tags created in the Guest Registration pane.
Define a Password Policy

In the Guest Management pane, use the Password Policy tab to configure requirements, such as minimum length or special character requirements, for passwords used by approved guests to log in to the network. These requirements are applied to:

- passwords that registering guests define for login
- system-generated network passwords for guest login

When defining the HTTP Login action, in the Guests tab, select the option **Provide a system-generated password to self-registering guests** to have Forescout platform generate passwords for guest login. For information about using system-generated passwords and providing a Forgot my Password link, refer to the Define Guest Login Session Options section.

To configure guest password requirements:


2. Define any of the following password requirements:
   - Minimum password length - the default, minimum length is 6 characters
   - Minimum number of uppercase characters to include
   - Minimum number of lowercase characters to include
Define a User Policy

In the Guest Management pane, use the User Policy tab to define how certain guest fields are validated.

The Email field is always mandatory for guests, and guests are identified by its contents.

- Clear the Allow invalid email addresses checkbox to ensure that this field contains a valid email address.
- In environments where guests are identified by information other than their email address, select the Allow invalid email addresses checkbox so that no validation is done on the field. Any value will be accepted in the Email field.

Create Sponsors

In the Guest Management pane, use the Sponsors tab to define the corporate employees who are authorized to log in to the Guest Management Portal. These users are called sponsors. Anyone defined as a sponsor can use the Guest Management Portal to approve, decline or revoke network access for their sponsored guests.

If the employee email address provided by a guest in the Guest Registration form is not defined in the Sponsors tab, the employee cannot use the Guest Management Portal. The employee can only approve or decline the guest if the Forescout user selected the Enable sponsor approval without authentication via emailed link option in the Guests tab of the HTTP Login action.

All sponsor email addresses must be configured in Active Directory.

Add sponsors in any of the following ways:

- Globally, by selecting all user directory members
- Individually, by defining an email address
• By group, by defining an Active Directory group

To configure sponsors:
1. Select the Sponsors tab of the Guest Management pane.

2. To add all corporate user directory domain members as sponsors, select the All domain members are sponsors option.

3. To add sponsors individually or by group:
   a. Select Add. The Add Sponsor dialog box opens.

   b. Define the following sponsor information:

<table>
<thead>
<tr>
<th>Email\Active Directory Group (required)</th>
<th>Define either of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Enter the Active Directory email address of the individual you want to define as a sponsor.</td>
</tr>
<tr>
<td></td>
<td>• Enter a corporate Active Directory group name to assign all its group members as sponsors.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type (required)</th>
<th>Select a sponsor type.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Sponsor - can access the portal to view and manage only guests that are assigned to them.</td>
</tr>
<tr>
<td></td>
<td>• Admin Sponsor - can access the portal to view and manage all guests that have registered for network access, and can override the statuses applied by other sponsors.</td>
</tr>
</tbody>
</table>
Enter a description for the Guest Management sponsor.

c. Select OK.

4. After all sponsors have been added, select **Apply** to save your changes in the configuration.

### Define Terms and Conditions

You can require users to agree to the use of your terms and conditions. In the Guest Management pane, use the *Terms and Conditions* tab to enable the presentation of terms and conditions to either or both of the following user types:

- Registering guests
- Sponsors working in the Guest Management Portal to manage guests

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

To configure terms and conditions:

1. Select the **Terms and Conditions** tab of the *Guest Management* pane.
2. Define the following:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable guest terms &amp; conditions</strong></td>
<td>Require terms and conditions to be confirmed by guests prior to their registering or logging in.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Provide the absolute URI of a Web page for displaying guest terms and conditions. Select <strong>Test</strong> to ensure that the address is correct.</td>
</tr>
<tr>
<td><strong>Text</strong></td>
<td>Define the text of terms and conditions to present to guests. Select <strong>Edit</strong> to add/modify/delete the terms and conditions, and select <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>Enable sponsor terms &amp; conditions</strong></td>
<td>Require terms and conditions to be presented to sponsors prior to them approving guest network access requests.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Provide the absolute URI of a Web page for displaying sponsor terms and conditions. Select <strong>Test</strong> to ensure that the address is correct.</td>
</tr>
<tr>
<td><strong>Text</strong></td>
<td>Define the text of terms and conditions to present to sponsors. Select <strong>Edit</strong> to add/modify/delete the terms and conditions, and select <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

3. Select **Apply** to save your changes.

**Guest Notifications**

In the Guest Management pane, use the **Guest Notifications** tab to configure which notifications Forescout platform sends to guests regarding their network access. Notifications can be sent to guests via email, SMS (text messaging), or both. 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 request network access
- By Forescout operators who register guests from the Forescout Console

**To configure guest notifications:**

1. Select the **Guest Notifications** tab of the *Guest Management* pane.

2. Define the following:

   Enable notifications to guests via:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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 notifications to guests.</td>
</tr>
</tbody>
</table>

   Notify guests when their guest account is set to:

<table>
<thead>
<tr>
<th>Account</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Pending</td>
<td>Notify guests that their network access request is pending.</td>
</tr>
<tr>
<td>Account Approval</td>
<td>Notify guests that their network access request has been approved.</td>
</tr>
<tr>
<td>Account Rejection</td>
<td>Notify guests that their network access request has been declined.</td>
</tr>
<tr>
<td>Account Revocation</td>
<td>Notify guests that their network access approval has been revoked. This state can only be triggered by a sponsor using the Guest Management Portal.</td>
</tr>
<tr>
<td>Account Expiration</td>
<td>Notify guests that their network access approval period has expired.</td>
</tr>
</tbody>
</table>

3. Select **Apply** to save your changes.

You can customize the notification texts. See [Localize Web Pages and Messages](#).

In the Guest Management Portal or the Network Access Request page opened by the emailed link, sponsors can add messages to guest notifications.
Sponsor Notifications

A corporate employee becomes a sponsor of a guest when one of the following conditions occurs:

- The registering guest specifies the person's email address in the Contact Person Email field of the Guest Registration form.
- The person's email address is provided in the Pre-defined sponsors for all guests field in the Guests tab of the HTTP Login action.
In the Guest Management pane, use the Sponsor Notifications tab to configure which notifications Forescout platform sends to sponsors regarding the following guest network access events:

- A guest registration request is pending for a guest for whom they are a sponsor.
- A guest registration request is approved for a guest for whom they are a sponsor.
- A guest registration request is rejected for a guest for whom they are a sponsor.
- A guest registration request is revoked for a guest for whom they are a sponsor. This event can only occur when a managing sponsor of the guest is working with the Guest Management Portal.

To configure sponsor notifications:

1. Select the Sponsor Notifications tab of the Guest Management pane.

2. Define when to notify a guest's sponsors:

| Account Pending | Notify the sponsors when a guest has requested network access. |
| Account Approval | Notify the sponsors when they approve a guest’s network access request. |
| Account Rejection | Notify the sponsors when they decline a guest’s network access request. |
| Account Revocation | Notify the sponsors when they revoke a guest’s network access. This state can only be triggered by a sponsor using the Guest Management Portal. |

3. Select Apply to save your changes.

You can customize the notification texts. See Localize Web Pages and Messages.
Sample Sponsor Email Notification

The following is a sample email sent to a sponsor regarding a pending guest request. The email contains the guest request details.

Support for Guest Management without Email Disclosure

By default, Forescout platform identifies each guest by their unique email address. If your organization does not want to require guests to share their email addresses, you can instruct Forescout platform to identify guests using other guest identification information.

Allowing 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. You can instruct Forescout platform to allow guests to enter other identification information.

To accommodate this new feature, the HTTP Login action, Registration Page tab includes a Full Name field that can be configured for Show/Hide/Mandatory:
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 IP range.

2. In the policy wizard Guest tab, ensure that the **Show a Login page link where guests can register for full network access as Logged 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 **Allow Invalid email addresses**.
  
  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.

- Select **Hide** from the **Full Name** dropdown menu.
  
  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>

**Allowing 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 Forescout platform 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>
</tbody>
</table>
The guest at email address '{0}' has been updated.  
<table>
<thead>
<tr>
<th>Label text</th>
<th>Update success message</th>
</tr>
</thead>
<tbody>
<tr>
<td>The portal already contains an Approved or Pending guest with email address...</td>
<td>Error text</td>
</tr>
<tr>
<td>Email address already exists. Can't override guest with status Approved...</td>
<td></td>
</tr>
</tbody>
</table>

**HTTP Login Action Configuration**

The HTTP Login action allows the Forescout operator to control the access of corporate and guest users to a corporate network. It is a powerful feature that can prompt endpoint users to authenticate or self-register before accessing your network. For information about how the action redirects endpoints, see [Endpoint Redirection](#).

When the HTTP Login action is enabled, users attempting to access the network are redirected to a Login page where they must enter valid credentials. The user credentials are authenticated against the CounterACT Appliance.

![Login page screenshot](image)

Use the *HTTP Login* action options to:

- Define the servers against which the user authenticates.
- Enable and define a registration process by which unauthorized users can request network access via a web registration form. You may want to enable this if your organization allows visitors to access the network.
Define login requirements so that users can skip authentication and registration, and enter the network with limited access.

**HTTP Login Action Configuration Tab**

The HTTP Login action can be used with other policy actions. For example, you can define a policy quarantining all unauthenticated users to an isolated VLAN. If the user logs in properly, the policy’s actions are cancelled. The user is removed from the isolated VLAN and can join the network and browse.

- **Web messages and emails used in this action can be changed and localized.** See [Localize Web Pages and Messages](#).
- **Login failures can be easily tracked.** See [Track Repeated Login Failures](#) for details.
- **You can customize the text that the HTTP Login action displays at the user’s endpoint.** For details, see [Customize HTTP Login Action Text](#).
- **HTTP Login is disabled whenever HTTP Redirection is disabled.** For more information, refer to the Forescout Administration Guide. See [Additional Forescout Documentation](#) for information on how to access this guide.

Depending on the endpoint operating system, and how the endpoint is managed, this action is implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin.

Configure the HTTP Login action to handle:

- **Guests:** See [Handling Guests](#)
- **Corporate users:** See [Handling Corporate Users](#)
Handling Guests

This section describes how to handle network guests. For example, you can create policies that deal with visiting professionals, contractors, etc.

You can configure the HTTP Login action so that users who do not have authentication credentials can register as network guests using a Guest Registration form that is displayed in the user's web browser. In the Login page, guests select Request access to open a Guest Registration form where they enter their contact details.

Sample Login Page and Guest Registration Form

The network access request is delivered to one or more corporate contacts ("sponsors") in your enterprise with the authority to approve network access. If approved, login credentials are automatically sent to the email address entered in the Guest Registration form.

To configure the HTTP Login action for guest registration and login, use the following tabs in the action configuration:

- **Guests Tab**: Defines how authentication and registration is performed.
- **Corporate Tab**: Defines which information guests must provide in the Guest Registration form.
- **Login Page Tab**: Defines the text that appears on the Login page.
- **Miscellaneous Tab**: Defines additional configuration options, such as encryption and compliance.
Handling Corporate Users
Use the Corporate options to enable corporate authentication.
To configure the action for corporate users, use the following tabs in the action configuration:

- **Corporate Tab**: Defines which servers are used for authentication.
- **Login Page Tab**: Defines the text that appears on the Login page.
- **Miscellaneous Tab**: Defines additional configuration options such as encryption and compliance.

HTTP Login Action Tabs
This section describes five of the HTTP Login action tabs.

Login Page Tab
The Login Page tab is used to define what is displayed on the Login page. This page appears for both guest and corporate users.

Sample Login Page
After the user successfully logs in, the endpoint's Authentication, Signed In Status property is resolved by Forescout platform as Signed In as a Guest if the user's status is network guest, or as Signed In as a Domain User if the user's status is corporate user.
The User Name entered here will be used when resolving the *Device Information > User Name* property. If necessary, you can instruct Forescout platform to use the machine name instead of this name or to use this name when the machine name is not available. Refer to the *HPS Inspection Engine Configuration Guide* for more information. See *Additional Forescout Documentation* for information on how to access this guide.

**HTTP Login Action, Login Page Tab**

The following Login Page tab options are available:

**Login Instructions**

In the text box of the Login Page tab, define the Login page message that is presented to both guests and corporate users.

**Show Help Button**

Help instructions are available on the Login page to assist users.

If you do not want to give users access to a Help page, hide the *Help* button on the Login page by clearing the *Show Help button* checkbox.
Guests Tab

Use the Guests tab to define guest login session options, as well as a registration strategy.

HTTP Login Action, Guests Tab

Guest Login Session Options

These options let you control the guest login experience.

HTTP Login Action, Guest Login Session Options

Enable HTTP login for approved guests

Select this option to enable login for approved guests. Authentication is validated against a Forescout server database after the guest is approved.

Keep open a 'Login Session' window after guest login

Select this option to display a corporate Login Session window for guests. To browse as a registered guest, the user selects Continue browsing in a new window and then OK.
Sample Corporate Login Session Window

The user must keep the Login Session window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, Forescout platform resolves the Authentication, Signed In Status property for the endpoint as Signed In as a Guest.

To leave the network, the user selects Log Out and then Leave.

Sample Logout Window
If the **Keep open a 'Login Session' window after guest login** checkbox is not selected, the corporate Login Session window is not displayed. Instead, a User Notification window is displayed. To browse as a registered guest, the user selects **Continue** and then **OK**. Forescout platform resolves the **Authentication, Signed In Status** property for the endpoint as **Not Signed In**.

**Sample User Notification Window**

**Allow each guest to be logged in concurrently on multiple endpoints**

You can control the number of devices a single guest can log in to concurrently. Select this option to allow multiple logins. If this option is not selected, a second login by the same user closes the first session on the original computer.

**Provide a system-generated password to self-registering guests**

Select this option to instruct Forescout platform to generate a password for the guest to use in the Password field of the Login page. This option is relevant only when a guest registers for network access using a Guest Registration form. When this option is selected:

- Guests are not prompted to define their own passwords in the Guest Registration form.
- When the guest is approved, Forescout platform generates a password for the guest to use in the Password field of the Login page.
- The system-generated password is provided in an email that is sent to the guest.

*System-generated passwords adhere to the password policy rules that are defined in the Guest Management pane's Password Policy tab. See Define a Password Policy.*
Enable guests to edit their profiles
Select this option to instruct Forescout platform to display the Edit Profile link in the Login page that is presented to guest users. Selecting this link displays the Edit Profile page, where guests can edit information that they initially provided when registering using the Guest Registration form.

Enable guests to request replacement passwords
Select this option to instruct Forescout platform to display the Forgot Password link in the Login page that is presented to guest users. Selecting this link displays the Forgot Password page, where approved guests can request a new password for login.

Guest Registration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a Login page link where guests can register for full network access as Signed-in Guests</td>
<td>Select this option to enable guests to self-register.</td>
</tr>
<tr>
<td>Set the Guest Registration page as the landing page for unregistered guests</td>
<td>Enables the Guest Registration page to be the default page for unregistered guests.</td>
</tr>
<tr>
<td>Limit guest accounts to:</td>
<td>Restricts guest access to specific hours.</td>
</tr>
<tr>
<td>Network access requests are automatically approved</td>
<td>Simplifies the approval process for guest access.</td>
</tr>
<tr>
<td>Guests must be approved by the sponsor they provide, or by:</td>
<td>Requires sponsorship approval for guest access.</td>
</tr>
<tr>
<td>Pre-defined sponsors for all guests</td>
<td>Pre-sets sponsors for all guests.</td>
</tr>
<tr>
<td>Sponsors must be in these domains:</td>
<td>Specifies domains for sponsor approval.</td>
</tr>
<tr>
<td>Enable sponsor approval without authentication via emailed link</td>
<td>Facilitates sponsor approval via email.</td>
</tr>
<tr>
<td>Require Verification Code</td>
<td>Requires verification code during guest registration.</td>
</tr>
</tbody>
</table>

Define Guest Registration Strategy

Allow only pre-approved guests
Clear the Show a Login page link where guests can register for full network access as Signed-in Guests checkbox if all guests must be pre-approved for network access. Information about pre-approved guests is saved on the CounterACT Appliance. When pre-approved guests log in to your network, their credentials are checked against this information. Pre-approved guests can be added by:

- a sponsor in the Guest Management Portal.
- a Forescout operator in the Guest Management Pane. It is the responsibility of your organization to forward login credentials to these pre-approved guests. Forescout platform does not do this.

Enable guest registration
To enable not-yet-approved guests to self-register, select the Show a Login page link where guests can register for full network access as Signed-in Guests checkbox. This prompts new guests to complete a Guest Registration form on which they provide information such as their identity details and the name of the individual who invited the guest to the network. A link to the Guest Registration form is provided on the corporate Login page.
**Landing page prompt**

Select **Set the Guest Registration page as the landing page for unregistered guests** if you want to prompt the guest to complete the Guest Registration form.

**Guest account expiration**

To set a maximum time for guests to request network access, select **Limit guest accounts to** and enter a time limit. When unspecified, the maximum network access approval period defaults to **eight hours**. In the Guest Management Portal, sponsors can set a specific limit to the network access of their self-registering guests. When the time period elapses, the guest account expires, and the guest is required to register again.

**Automatic approval of registered guests**

To automatically approve guests after submitting a Guest Registration form, select **Network access requests are automatically approved**. You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who is registered. Approved guests are displayed in the following ForeScout platform locations:

- In the Guest Management Portal where sponsors can view the registered guests that specified them as their corporate contact.
- In the Guest Registration Pane. Select **Options** from the **Tools** menu and then navigate to and select **Guest Registration** to display the **Registered Guests** tab and view the registered guest entries.

**Sponsor approval of guests**

If you require that guests be explicitly approved by an individual in your organization - a corporate **sponsor** - select the **Guests must be approved by the sponsor...** option. The sponsor specified by the guest on the Guest Registration form receives a notification email that includes a link to the corporate Guest Management Portal. After logging in to the portal, sponsors can approve or decline network access to their guests awaiting approval.

Before sponsor approval is completed, a notification page opens for the guest.
Enable sponsor approval without authentication via emailed link

The guest registration request notification email that is sent to sponsors always includes a link to the corporate Guest Management Portal. Select this option to include an additional link in the notification email to a Network Access Request page containing the specific guest registration request.
The first link opens the Login page of the Guest Management Portal, where a sponsor can log in and administer all their guest registration requests.

If the Forescout user selected the Enable sponsor approval without authentication via emailed link option in the Guests tab of the HTTP Login action, then a second link is included. This link opens a Network Access Request page, where the sponsor can approve or decline the network access request of the specific guest.

Sample Network Access Request - Sponsor Approval Page

This option is useful if:

- You do not want to require sponsors to log in to the Guest Management Portal to approve guest registration requests.
- Sponsors are temporarily unable to access the Guest Management Portal.
- Your organization does not employ an Active Directory server to verify the credentials of its personnel. (Logging in to the Guest Management Portal requires Active Directory verification of user domain credentials).

Use of this option maintains backward compatibility with HTTP Login action functionality of previous versions.

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.
**Pre-defined sponsors for all guests**

Select this option to provide a comma-separated list of emails of corporate sponsors. In addition to the primary sponsor named by each guest in the Contact Person and the Contact Person Email fields of the Guest Registration form, these sponsors will also receive guest registration notifications.

**Sponsors must be in these domains**

To make the approval process more scalable, your network guests can be approved by individuals in your organization, based on the domain address of the Contact Person Email that they entered in the Guest Registration form.

Select this option to provide a comma-separated list of corporate domains. The entries specified in this field limit the allowed domain(s) in the Contact Person Email field of the Guest Registration form submitted by a registering guest. For example, if the field contains the entries **finance.my-company.com, marketing.my-company.com, sample.com**, then only an email address that ends with one of these domains, such as **jane@marketing.my-company.com**, is valid for use in the Contact Person Email field.
Require Verification Codes

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 Guest Registration form is valid. Forescout platform 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. Verification codes are automatically generated and validated by Forescout platform.

Sample Guest Verification Code Form

Verification codes are automatically generated and validated by Forescout platform.

To work with verification codes:

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. The email messages includes a customized message. The mobile text message includes only the verification code.

To send a verification code to a mobile device, you must define how Forescout platform submits the message to the mobile carrier.
To define text messaging through a mobile carrier:

1. Select **Options** from the Console **Tools** menu and then select **General > Mobile Text Message**.

   ![Mobile Text Message Pane](image)

   **Mobile Text Message Pane**

2. Select **Add**. The **Carrier Type** dialog box opens.

   ![Mobile Text Message Carrier Type](image)

   **Mobile Text Message Carrier Type**

   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.
Mobile Text Message Request, Email Format

- 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.

Mobile Text Message Request, URL Format

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.

**Viewing Registered Guests**

Approved and unapproved guests can be viewed in the Guest Management Portal and in the Guest Registration Pane.

**Working with Guest Tags**

Use guest tags to categorize guests into groups; for example, *Conference* guests and *Contractor* guests or *Building A* guests and *Building B* guests.

You can create policies that evaluate guests for their guest tag assignments. For example, create a policy that detects *Conference*-tagged guests and assigns them to a specific VLAN or allows them minimum network access.

See [Configure Tags](#) for detailed information about working with guest tags.

**Corporate Tab**

Use the Corporate tab to define which servers will be used for domain authentication, as well as other authentication settings.

Before configuring corporate users, you must have already configured User Directory servers. Under most circumstances this configuration was performed when setting up the Console using the Initial Setup wizard.

To see which servers are defined, select **Options** from the Console **Tools** menu and then select **User Directory**. For more information about configuring User Directories refer to the *Forescout User Directory Plugin Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

**HTTP Login, Corporate Tab**

To enable corporate user authentication against an authentication server, select **Enable HTTP login for corporate users**.
To allow authentication against any of the authentication servers that you defined in the User Directory Plugin, select **Use any authentication server**.

To authenticate users against specific servers, select **Use specific authentication server** and then select the browse button to choose servers.

![HTTP Login, Defined Authentication Servers](image)

**HTTP Login, Defined Authentication Servers**

To allow the endpoint user to select a server against which to authenticate, select **Prompt users to select an authentication server**. When this option is selected, the Login page displays a Domain field, from which the endpoint user can select a domain.

![Sample Login Page with Domain](image)

**Sample Login Page with Domain**

To display a corporate Login Session window for corporate users, select the **Keep open a 'Login Session' window after guest login** option. The user must keep this window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, Forescout platform resolves the **Authentication, Signed In Status** property for the endpoint as **Signed In as a Domain User**.
Control the number of machines a single user can log in to concurrently. Select **Allow each guest to be logged in concurrently on multiple devices** to allow multiple logins. If this option is not selected, a second login by the same user closes the first session on the original computer.

To speed up the login process in multi-domain networks, select **Require the User Name to include the domain**. This requires corporate users to provide their domain name during authentication.

**Registration Page Tab**

The information in the *Registration Page* tab is only used if *guest registration is enabled* in the *Guests* tab.

Use the *Registration Page* options to design the *Guest Registration* form.

**HTTP Login, Sample Guest Registration Form**

- Define the title and message that appears in the *Guest Registration* form.
- Define the form fields that you want guests to use.
Require guests to enter a registration code to begin the registration process. (optional)

HTTP Login, Registration Page Tab

**To design the Guest Registration form:**

1. In the **Header** field define a Guest Registration form title.

2. In the Registration Instructions text box, define the message that will appear in the page.

3. Select **Use registration code** to require guests to enter a registration code before beginning the registration process. This ensures that only guests with whom you’ve shared a registration code can apply for network access. These codes are automatically generated by Forescout platform, but they must be shared with endpoint users manually. See [Retrieving Registration Codes](#).

4. Select **Enable automatic login without a password** if you want to allow users to log in without a password. When this checkbox is selected, there is no authentication.

5. The **Email** field is always mandatory, and guests are identified by its contents.
   - Clear the **Disable email validation** checkbox to ensure that this field contains a valid email address.
In environments where users are identified by information other than their email address, select the **Disable email validation** checkbox so that no validation is done on the field. Any value will be accepted in the **Email** field.

To ensure that only one guest identification field is displayed in the Guest Registration form, it is recommended to set the **Full Name** dropdown menu to **Hide** whenever the **Disable email validation** checkbox is selected.

6. For each field in the list, select one of the following:
   - **Hide**: The field is not displayed in the Guest Registration form.
   - **Show**: The field is displayed in the Guest Registration form and is optional.
   - **Mandatory**: The field is displayed in the Guest Registration form, and the user must enter a value.

7. If tags are defined in your environment, you can select tags to be added to the Guest Registration form.

   SMS must be disabled to hide the Phone field on the Guest Registration page. See Guest Management Pane.

The list of fields includes five custom fields that you can configure. For example, **Custom1** might be renamed **Building Name** to indicate the name of the building where the guest is located.

**To assign custom names:**

1. Select **Options** from the **Tools** menu and then select **Advanced > Language Localization > Endpoint Messages**.

2. Type the word **Custom** in the search field.

   ![Localization](image)

3. Edit the fields as required, and then select **Apply**.

For more information, see [Localize Web Pages and Messages](#)
**Miscellaneous Tab**

Use the Miscellaneous tab to configure additional user login parameters.

![HTTP Login, Miscellaneous Tab](image)

**Use encrypted protocol (HTTPS)**

It is recommended to select the **Use Encrypted protocol (HTTPS)** checkbox to send the Login page via HTTPS. To send it via the non-encrypted HTTP protocol, clear the **Use Encrypted protocol (HTTPS)** checkbox. For more information about this transmission method, refer to the *Transmitting Actions via HTTPS* section in the *Forescout Administration Guide*. See *Additional Forescout Documentation* for information on how to access this guide.

**Direct user to a predestinated site after successful login**

To force the user to begin browsing at a specific website, such as your corporate home page, select **After a successful login continue to this URL** and enter the URL.

**Allow user to skip login and have internet access only**

If you think login credentials may not be available to users, and you want them to have browsing access, select **Allow the user to skip login and have internet access only**. When selected, the Login page includes a guest link option.

**Attempt to open a browser at the endpoint**

You can configure the action to automatically open a browser at the endpoint, instead of waiting for the user to browse. This ensures that the HTTP message gets to the network user faster. Select **Attempt to open the endpoint browser**. (This option is for managed machines only, and is not available for Windows 2000 and Windows 2003 Server machines.) Forescout platform uses a script when this option is selected.

Refer to the *HPS Inspection Engine Configuration Guide* for details about how scripts work. See *Additional Forescout Documentation* for information on how to access this guide.

**Do not redirect endpoint browser session**
If the previous option **Attempt to open the endpoint browser** is selected together with this option, the Login page opens as a new page. If the **Attempt to open the endpoint browser** option is not selected together with this option, endpoint users must right-click the desktop **SecureConnector** taskbar icon, and select **View Compliance Center** to view the page. Hosts must be managed.

### Customize HTTP Login Action Text

You can customize text that the **HTTP Login** action generates at the user endpoint. These texts appear in re-directed HTML pages that are generated at endpoints of users who attempt to access the corporate network.

See [Localize Web Pages and Messages](#). You can identify **HTTP Login** action texts in the Endpoint Messages pane by any one of the following Action column entries:

- Guest verification code
- HTTP Login (with or without other values)
- HTTP Login mobile

### Track Repeated Login Failures

You can define the number of failed attempts within a time range that trigger tracking. In addition, you can follow up with users who exceeded the limit by creating useful policy actions, for example, notifying the IT team or preventing user access to the production network.

**To track repeated login failures:**

1. Select **Options** from the Console **Tools** menu and then select **NAC > HTTP Login Attempts**.

![Options](options.png)

2. Set the number of failed logins attempts and the time within which failed login attempts must occur for a login failure attempt to be detected.

3. Select **Apply**.
Endpoint Redirection

When Forescout platform detects web traffic from unauthorized endpoints, it can run an HTTP Login action to redirect (hijack) the traffic to a captive portal, such as a Login page.

Hijack Methods

Forescout platform provides three guest endpoint redirection methods for guest management purposes. These methods can be deployed individually or in any combination.

- Centralized Web Authentication Method
- Packet Engine Method
- DNS Enforce Plugin Method

Centralized Web Authentication Method

Forescout platform centralized web authentication combines the use of both MAC authentication (provided by the RADIUS Plugin) and Forescout policy actions to authenticate endpoints.

As of RADIUS Plugin version 4.2, Forescout platform’s hijack capability is not dependent on any other plugin or feature.
Packet Engine Method
The Forescout Packet Engine can be used to hijack the user’s HTTP session.

- This method is not recommended for encrypted traffic.

DNS Enforce Plugin Method
The Forescout DNS Enforce Plugin can be used to redirect the user’s session to a captive portal.

- This method is not recommended when background apps, such as Outlook Client, attempt to connect to their servers.

Advanced Redirection Configuration
Refer to Management and Corporate User Login How-to Guide for advanced HTTP traffic handling preferences.
Guest Management Interface Customization

You can customize texts and the look-and-feel of several Forescout features, including the Guest Management Portal.

Localize Web Pages and Messages

You can edit or localize text, such as error messages, email messages and labels, that appear in several Forescout features.

To edit or localize text:

1. Select Options from the Tools menu and then select Advanced > Language Localization > Endpoint Messages.

   The table lists text strings that Forescout platform displays in various interactions with a detected endpoint.

2. In the search field of the Endpoint Messages pane, enter any portion of the text that you want to localize. For example, 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.

3. Select the row with the text you want to change, and select Edit. The Edit Locale Text dialog box opens and displays the text of the selected entry.
4. Enter the new text, and select **OK**.

   Select a table entry and then select **Default** to return to the default text.

5. When you are done editing the texts, select **Apply**.

**The Forescout User Portal Builder**

Use the Forescout User Portal Builder to customize the following Forescout user interfaces:

- HTTP Notification
- HTTP Login
- Guest Management Portal

The legacy Customization Tool is still used for customizing the interfaces for HTTP Localhost Login, Start SecureConnector, Start Macintosh Updates, Start Windows Updates, Windows Self Remediation and Compliance Center. For more information about the legacy Customization Tool, refer to the Forescout Administration Guide. See [Additional Forescout Documentation](#) for information on how to access this guide.

When using the User Portal Builder, each skin is responsive to laptop/PC mode, tablet mode, and mobile device mode. There is no unique customization for mobile devices.
Opening the User Portal Builder

To open the User Portal Builder, do one of the following:

- Select **Options** from the Console **Tools** menu, navigate to **NAC > HTTP Redirection**, and select **Open** User Portal Builder.
In the Console, select the Ellipsis icon from the Toolbar menu, and select User Portal Builder.

Using the User Portal Builder to Customize Skins

The User Portal Builder includes an out-of-the-box default skin for each of the Forescout user interfaces.

Each Forescout user interface has its own type of skin. You can customize a skin in different ways:

- **Basic Customization**
- **Advanced Customization**

**Basic Customization**

The User Portal Builder provides a simple way to edit and preview:

- the color settings of the most commonly-customized fonts
- the color settings of the most commonly-customized background areas and buttons
- the logo

New skins can be added, and skins that were added can be edited.

To add a new skin:

1. In the User Portal Builder, select **Add**.
2. Select the user interface:
   - Add HTTP Login Skin to customize the HTTP Login window.
   - Add HTTP Notification Skin to customize the HTTP Notification window.
   - Add Guest Management Skin to customize the Guest Management Portal.

3. A copy of the default skin opens for you to edit.

4. Edit the skin colors and logo as needed, and assign a name to the new skin.

   Uploaded logo files must be in PNG format and cannot be larger than 1 MB.
5. Name the skin, and select **Save** to save it to the User Portal Builder.

**Advanced Customization**

You may want to configure user interface features that are not included in the User Portal Builder basic customization. For example:

- Fonts and font sizes
- Field shapes and positions
- Background images

**To edit customized features:**

1. In the *Add Skin* page, select **Use a CSS file**.

2. Select **Download the default CSS template** to download the CSS file of a pre-defined skin template. (Optional)

3. Edit the downloaded skin or a skin that has been previously added.
4. When you are done editing the CSS file, select the **Upload CSS** button to upload it to the User Portal Builder.

*The User Portal Builder cannot be used to localize user interface text. To localize the text, see [Localize Web Pages and Messages](#).*

### Deploying a Skin for a User Interface

Exactly one skin is deployed throughout your network for each type of user interface. In the User Portal Builder, select the skin to be deployed in place of the one currently deployed, and then select **Deploy**.

---

**Additional Forescout Documentation**

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

#### Documentation Downloads

Documentation downloads can be accessed from the [Forescout Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

*Software downloads are also available from these portals.*
To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

To access documentation on the Customer Support Portal:

- Go to https://Forescout.force.com/support/ and select Downloads.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select Administration Guide from the Help menu.
**Plugin Help Files**

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin and then select **Help**.

**Documentation Portal**

- Select **Documentation Portal** from the **Help** menu to access the [Documentation Portal](#).