



# Forescout

## Authentication Module: User Directory Plugin

### Server and Guest Management Configuration Guide

Version 6.5.1



## 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](mailto: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.

2020-07-27 13:24

# Table of Contents

<b>Preface</b> .....	<b>5</b>
Authentication Module Information .....	5
Additional Forescout Documentation .....	6
Documentation Downloads .....	6
Documentation Portal .....	7
Forescout Help Tools.....	7
 <b>Chapter 1: User Directory Management</b> .....	<b>8</b>
Endpoint User Details.....	8
Endpoint Authentication .....	8
User Directory Inventory .....	9
Related Documentation .....	9
Supported Servers .....	9
Requirements .....	10
Ensure That the User Directory Plugin Is Running .....	10
Configuration .....	11
Configuring Servers to Work with Certificates .....	11
Define Servers .....	12
Advanced Settings Configuration Tab .....	23
Duplicate Servers .....	27
Test the Configuration .....	27
Working with Policies .....	28
Detect Endpoints with User Directory Attributes .....	28
Display User Directory Information at the Console .....	29
Additional Information .....	31
DNS Detection for Microsoft Active Directory.....	32
Compatibility Across Servers.....	33
 <b>Chapter 2: Corporate and Guest Management</b> .....	<b>35</b>
Corporate and Guest Control .....	35
Corporate/Guest Control Policy .....	35
Groups Populated by a Corporate/Guest Control Policy .....	36
Using the Corporate/Guest Control Policy Template .....	37
What to Do When Authentication Server Values Are Changed .....	42
Report Generation .....	42
Guest Management from Portal and Console .....	43
Guest Management Portal .....	45
Guest Management Pane .....	46
Support for Guest Management without Email Disclosure .....	62
HTTP Login Action Configuration.....	67
Handling Guests.....	69
Handling Corporate Users .....	70
HTTP Login Action Tabs .....	70
Customize HTTP Login Action Text .....	89
Track Repeated Login Failures.....	89

Endpoint Redirection.....	90
Hijack Methods .....	90
Guest Management Interface Customization .....	91
Localize Web Pages and Messages.....	91
The Forescout User Portal Builder .....	93

## Preface

The User Directory Plugin is a component of the Forescout Authentication Module. See [Authentication Module Information](#) for details about the module.

The User Directory Plugin resolves endpoint user details and defines the authentication and directory servers used for endpoint authentication. A real-time display of network information at multiple levels, including user directory information, is available from the Console.

The plugin also enables a variety of other features for handling network guests and the sponsors who approve guest access to the network. These features are described in the *Guest Management Portal How-to Guides* for sponsors and Forescout operators, and in the *Forescout Administration Guide*.

The plugin is comprised of two components:

- [Chapter 1: User Directory Management](#)
- [Chapter 2: Corporate and Guest Management](#)

## Authentication Module Information

The Forescout Authentication Module provides secure network access across wired, wireless, and guest networks through its RADIUS and User Directory Plugins.

The Authentication Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean Forescout installation.

The User Directory and RADIUS Plugins are installed and rolled back with the Authentication Module.

Refer to the *Forescout Authentication Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

## 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 [Technical Documentation Page](#), and from 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**.

### Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

**To access the Technical Documentation page:**

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

### Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides 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 product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation 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/](https://updates.forescout.com/support/files/counteract/docs_portal/)

## Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Forescout Console.

### *Console Help Buttons*

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

### *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**.

### *Content Module, eyeSegment Module, and eyeExtend Module Help Files*

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

### *Documentation Portal*

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

# Chapter 1: User Directory Management

## Endpoint User Details

The User Directory Plugin is used to resolve an extensive range of endpoint details, for example, the LDAP display name, department name, and email addresses. This information is displayed in the Detections pane and in other Console windows.

The screenshot shows the Forescout console interface. The top navigation bar includes 'File', 'Reports', 'Actions', 'Tools', 'Log', 'Display', and 'Help'. Below this is the 'FORESCOUT' logo and a navigation menu with 'Home', 'Asset Inventory', 'Policy', and a settings icon. The main content area is titled 'All Hosts' and shows a table of endpoints. The table has columns for Host, IPv4 Address, Display Name, Department, Email, and Phone. Three endpoints are listed: DOM311Q..., DOM321Q..., and DOM321Q... with details like 'Fay Lomain', 'Dan Aclay', and 'Raul Polly'.

Below the table, there is a 'Profile' tab and a 'User' section. The 'User' section displays details for a user named 'administrator' with IP address 'IPv4'. The details include: Address: 10.10.10.10, Hostname: QA-EAF61583C255, Function: Computer, MAC Address: 0050569F5028, Domain: DOM31, and Operating System: Windows XP Professional.

The 'User' section also includes a 'General' tab and a 'Security' tab. The 'General' tab shows fields like 'Account is Disabled', 'Account is Expired', 'Company', 'Department', 'Display Name', 'Distinguished Name', 'Email', 'Employee Number', 'Initials', 'Last Name', 'LDAP User Name', and 'Member Of'. The 'Security' tab shows fields like 'Mobile Phone', 'Password Last Set', 'Phone', 'Street Address', and 'Title'.

See [Detect Endpoints with User Directory Attributes](#) for details.

## Endpoint Authentication

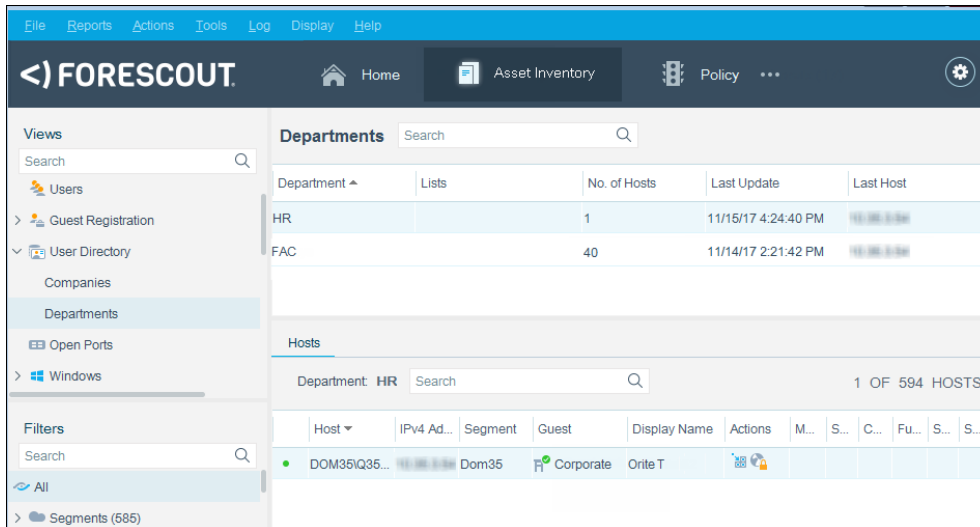
Use the HTTP Login action to prompt endpoint users to authenticate.

You can define the action so that users at guest hosts and guests are prompted to register with the network before receiving valid credentials. Users are presented with a Login page at each attempt to access the network. A valid user name and password must be entered. Refer to the *Forescout Administration Guide* for more information. See [Additional Forescout Documentation](#) for information on how to access the guide.



## User Directory Inventory

The Console Asset Inventory view presents a real-time display of network information, including user directory information, at multiple levels.



Refer to the *ForeScout Administration Guide* for information about working in the Asset Inventory view. See [Additional ForeScout Documentation](#) for information on how to access the guide.

## Related Documentation

Refer to the *Guest Management Portal How-to Guides* for information about working with the portal. See [Additional ForeScout Documentation](#) for information on how to access the guide.

Refer to the *ForeScout Administration Guide* for information about working with:

- The HTTP Login action. This action is used to prompt guest registration.
- The Guest Registration feature. This feature is used to define guest parameters, such as password policies or automated sponsor and guest notifications.

## Supported Servers

The following user directory and authentication servers are supported:

- Microsoft Active Directory
- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP Server
- RADIUS

- TACACS

You can work with more than one server type simultaneously. For example, if your organization uses Microsoft Active Directory for retrieving user details and a RADIUS server for verifying authentication, you can configure the plugin to work with both these server types.

## Requirements




The plugin requires the following:

- Forescout version 8.2.1
- Appliance or Enterprise Manager access to the User Directory servers.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

## Ensure That the User Directory Plugin Is Running

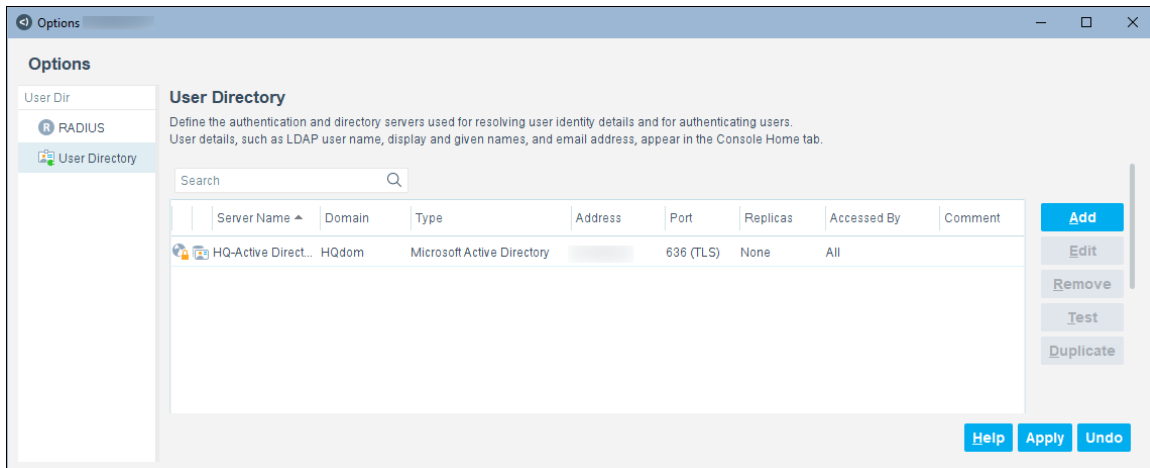
After installing the User Directory Plugin (and configuring it, if necessary), ensure that it is running.

### To verify:

1. Select **Tools > Options > Modules**.
2. In the *Modules* pane, hover over the User Directory Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.  
The name is preceded by one of the following icons:
  -  - The User Directory Plugin is stopped on all Forescout devices.
  -  - The User Directory Plugin is stopped on some Forescout devices.
  -  - The User Directory Plugin is running on all Forescout devices.
3. If the User Directory Plugin is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

## Configuration

A basic User Directory server configuration was most likely carried out via the Console Initial Setup Wizard, which opens the first time you log in to the Console. The server configuration defined in the Wizard automatically appears in the User Directory pane of the Options window.



You can connect additional User Directory servers to Forescout components, and define user and domain credentials, replica servers, and other parameters. The configuration can also be tested.

Procedures for defining additional server configurations are described in this document. To edit an existing configuration, select the configuration and then select **Edit**.

### Access to Servers

User scopes are managed by users defined as administrators in the *CounterACT User Profile* pane (**Tools > Options > CounterACT User Profiles**). If you do not have the required permissions to configure User Directory servers or to work with the IP addresses assigned to them, you receive an error message when attempting configuration. Contact your CounterACT Administrator if required.

## Configuring Servers to Work with Certificates

To ensure secure communication, Forescout platform can:

- Verify certificates presented by external services and applications
- Present system certificates to external services and applications for authentication

### To configure the plugin to use certificates:

1. Select **Options** from the Console **Tools** menu.
2. In the *Options* pane, select **Certificates**, and ensure that system and trusted certificates are configured for this scope.
3. In the *User Directory Communication* settings, set the server port to **636** (or any port configured for secure communication), and select **Use TLS**.

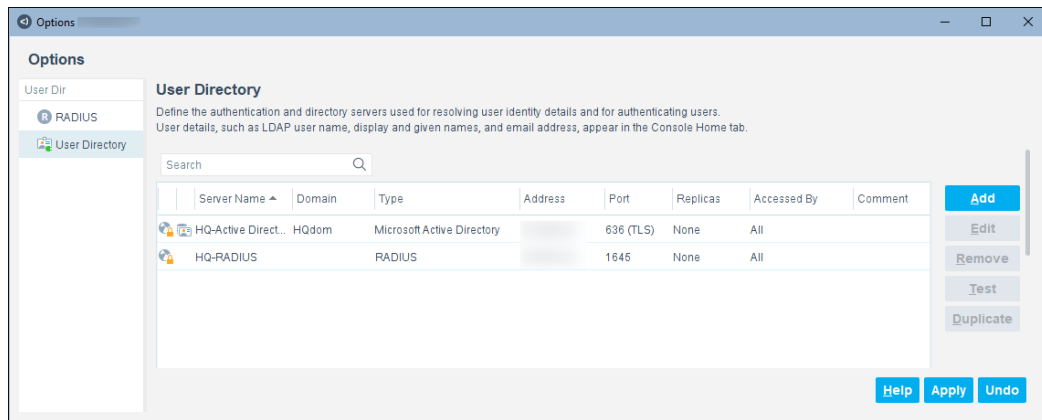
4. Complete the server definitions.
5. After the server is defined, select the server, select **Edit > Advanced**, and configure the certificate settings.

## Define Servers

This section describes how to define User Directory servers.

**To add or edit User Directory servers:**

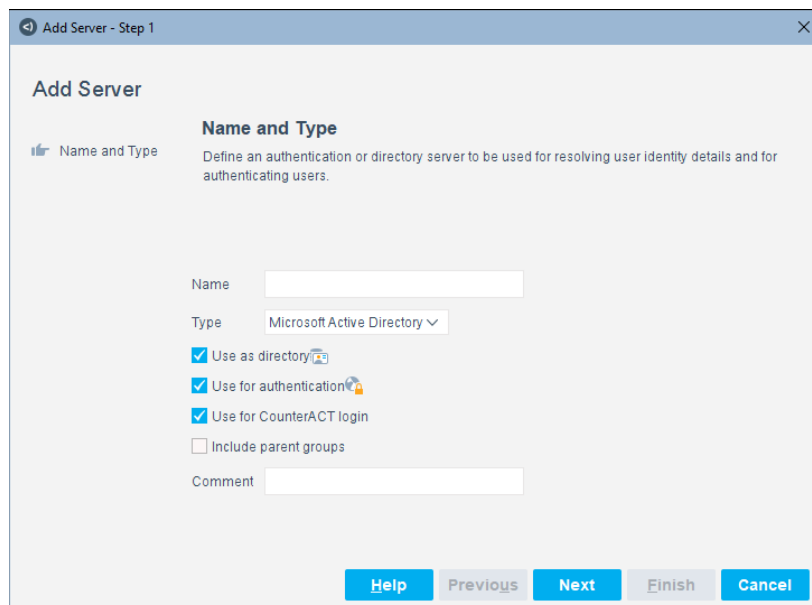
1. Select **Options** from the Console **Tools** menu.
2. In the *Options* pane, select **User Directory**.



3. Select **Add**, or select an existing server configuration and select **Edit**. The Server wizard opens to the Name and Type pane.


## Configure the Name and Type

The server type is configured in the *Name and Type* step of the *Add Server* wizard.



Configure the following settings in this pane:

<b>Name</b>	Enter the hostname of the server. <b>Note:</b> <i>This value cannot be edited.</i>
<b>Type</b>	Select a server type. The wizard displays the configuration parameters for the selected server type. <b>Note:</b> <i>This value cannot be edited.</i>
<b>Use as directory</b>	Select this option to use the server as a directory to retrieve user information. This option is not available for RADIUS and TACACS servers.
<b>Use for authentication</b>	Select this option to use the server for user authentication.
<b>Use for CounterACT login</b>	Select this option to use the server for user authentication when logging in to the Forescout Console or Is.
<b>Include parent groups</b>	This option is available for Microsoft Active Directory server type only. Select this option to detect the group that the user is a member of, as well as parent groups. Policies with the <i>User Directory &gt; Member Of</i> property resolve this information.
<b>Comment</b>	Enter comments if required.

 The plugin does not support enabling both of the following settings at the same time:

- [Include parent groups](#) setting
- [Targeted Group Resolution](#) advanced setting

Attempting to apply such a configuration fails.

4. Select **Next**.

## Configure Server Settings

The parameters included in the Settings pane of the Add Server wizard vary, depending on the selected server type and the enabled plugin features.

### [Communication Settings](#)

This section describes the server communication details required regardless of the server type used.

**Add Server**

**Settings**  
Define the Microsoft Active Directory server parameters. CounterACT will use these parameters to communicate with the server.

**Communication**

Address  ☐ DNS Detection

Port  ☒ Use TLS

Accessed By ☒ All CounterACT Devices (Recommended)  
☐ Enterprise Manager

Directory

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

<b>Address/DNS Detection</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Enter the remote address of the server, such as an IP address, FQDN address string, or IPv6 address string. For server types other than Microsoft Active Directory, this is the only option.</li> <li>Select <b>DNS Detection</b> to instruct Forescout platform to learn directory servers based on the domain name that you configure in the <b>Domain</b> field in the <b>Directory</b> section. In the User Directory table, the Address value is dynamically learned. This option applies to Microsoft Active Directory servers only. For details, see <a href="#">DNS Detection for Microsoft Active Directory</a>. You can later change how often the plugin queries for domain controller addresses. See <a href="#">DNS Detection Refresh Interval</a>.</li> </ul>
<b>Port</b>	<p>Enter the server port:</p> <ul style="list-style-type: none"> <li>For RADIUS servers, the default port is 1645.</li> <li>For TACACS servers, the default port is 49.</li> <li>For all other servers, the default port is 636.</li> </ul>
<b>Use TLS</b>	<p>For some server types, you can instruct Forescout platform to use TLS to encrypt communication with the User Directory server. By default, <b>Use TLS</b> is enabled.</p> <p>Ensure that TLS communication is supported and enabled on servers used as directories to retrieve user information. By default, the User Directory Plugin enables communication with servers that support TLS 1.1 or TLS 1.2 only. To enable communication with servers that support TLS 1.0 only, see <a href="#">TLS 1.0 Communication Configuration</a>.</p>
<b>Accessed By</b>	<p>Select which CounterACT devices can communicate with the server. The <i>All</i> option is recommended as it enables faster resolution. If you select <b>All</b>, make sure that all CounterACT Appliances have access to the server being configured.</p>

### *TLS 1.0 Communication Configuration*

By default, the User Directory Plugin can only communicate with servers using TLS if they use TLS 1.1 or TLS 1.2. You can enable TLS 1.0 communication, but this is not recommended because it is less secure.

TLS 1.0 communication needs to be configured on each CounterACT device.

#### **To enable TLS 1.0 communication on a CounterACT device:**

1. In the CLI, run the following command:

```
fstool ad set_property config.tls.versions.list tlsv1_2,tlsv1_1,tlsv1
```

2. Run the following command:

```
fstool ad get_property config.tls.versions.list
```

The following is displayed:

```
config.tls.versions.list = tlsv1_2,tlsv1_1,tlsv1
```

3. Run the following command:

```
fstool ad restart
```

#### **To disable TLS 1.0 communication on a CounterACT device:**

1. In the CLI, run the following command:

```
ad set_property config.tls.versions.list tlsv1_2,tlsv1_1
```

2. Run the following command:

```
fstool ad get_property config.tls.versions.list
```

The following is displayed:

```
config.tls.versions.list = tlsv1_2,tlsv1_1
```

3. Run the following command:

```
fstool ad restart
```

### *Microsoft Active Directory Server Settings*

This section describes the server details required when working with Microsoft Active Directory Server. These settings are configured in the Settings pane of the Add Server wizard.

**Add Server - Step 2 of 4**

**Add Server**

✓ Name and Type  
 Settings  
 Test  
 Replicas

**Settings**  
 Define the Microsoft Active Directory server parameters. CounterACT will use these parameters to communicate with the server.

**Directory**

Domain   
[Example: Fully Qualified Domain Name, e.g. MyCompany.com]

Administrator

Password

Verify Password

**Additional Domain Aliases**

☒ None  
☐ Any  
☐ Specify   
[Example: Subdomain, e.g. REMOTE for remote.mycompany.com]

Help Previous Next Finish Cancel

For a description of the Communication settings, see [Communication Settings](#).

Configure the following additional server settings in the *Directory* and *Additional Domain Aliases* sections:

<b>Domain</b>	<p>The domain name (e.g., MyCompany.com).</p> <p>When <b>DNS Detection</b> is selected in the <a href="#">Communication Settings</a>, the plugin uses this domain name to automatically learn the addresses of directory servers.</p> <p>Domain name restrictions:</p> <ul style="list-style-type: none"> <li>The domain name may contain up to 63 characters.</li> <li>The domain name may contain:             <ul style="list-style-type: none"> <li>alphanumeric characters</li> <li>any of the following special characters: ! @ # \$ % ^ &amp; ( ) - _ ' { } . ~</li> </ul> </li> <li>The domain name may <i>not</i> contain:             <ul style="list-style-type: none"> <li>empty spaces</li> <li>a period (.) as the first character</li> <li>any of the following special characters: \ * + =   : ; , " ? &lt; &gt;</li> </ul> </li> </ul>
<b>Administrator</b>	The credentials to authenticate to the directory for querying other user details.
<b>Password</b>	The Administrator's password.



<b>Additional Domain Aliases (optional)</b>	<p>Alternative names for the domain being configured.</p> <p><b>None:</b> A user is looked up in this directory only if its domain name matches the directory domain defined in the <b>Domain</b> field.</p> <p><b>Any:</b> A user is looked up in this directory regardless of the user's domain name.</p> <p><b>Specify:</b> Specify a comma-separated list of domain names. A user is looked up in this directory if its domain name matches one of the listed domain names or the configured directory domain name.</p>
---	---

### *Novell eDirectory, Oracle Directory, IBM Lotus Notes and OpenLDAP Server Settings*

This section describes the details required when working with the following servers:

- Novell eDirectory
- OpenLDAP Server
- IBM Lotus Notes
- Oracle Directory Server

**Add Server - Step 2 of 4**

**Add Server**

**Settings**  
Define the Novell eDirectory server parameters. CounterACT will use these parameters to communicate with the server.

**Communication**

Address:

Port:  ☒ Use TLS

Accessed By: ☒ All CounterACT Devices (Recommended)  
☐ Enterprise Manager

**Directory**

Base DN:   
*[Example: ou=MyDepartment,ou=user,o=MyCompany]*

Administrator Bind DN:   
*[Example: cn=admin,ou=user,o=MyCompany]*

Password:

Verify Password:

Authentication Bind DN Pattern:   
*[Example: cn=[user],ou=user,o=MyCompany]*

**Additional Domain Aliases**

☒ None  
☐ Any  
☐ Specify   
*[Example: ou=People,dc=myfab,dc=com]*

**Help Previous Next Finish Cancel**

You may need to perform advanced configurations when working with these servers. See [Advanced Settings Configuration Tab](#).

For a description of the Communication settings, see [Communication Settings](#).

Configure the following additional server settings in the *Directory* and *Additional Domain Aliases* sections:

<b>Base DN</b>	The root of the LDAP directory tree where users should be looked up.
<b>Administrator Bind DN</b>	The Bind DN of a user allowed to look up other users in the directory.
<b>Password</b>	The Administrator's password.
<b>Authentication Bind DN Pattern</b>	<p>The pattern used to construct a Bind DN string when authenticating a user to the server. The pattern must contain the string <code>{user}</code>, which is replaced by the username during each authentication request.</p> <p>Example: <code>CN={user},ou=user,o=MyCompany</code></p>
<b>Additional Domain Aliases (optional)</b>	<p>Alternative names for the domain in which to look up users.</p> <p><b>None:</b> The user is looked up in this directory only if the endpoint's domain name matches the domain name of this directory.</p> <p><b>Any:</b> The user is looked up in this directory regardless of the endpoint's domain name.</p> <p><b>Specify:</b> Specify a comma-separated list of domain names. The user is looked up in this directory if the endpoint's domain name matches the domain name of this directory or a name in the list.</p>

### RADIUS Server Settings

This section describes the details required when working with RADIUS.

**Add Server - Step 2 of 4**

**Add Server**

**Settings**

Define the RADIUS server parameters. CounterACT will use these parameters to communicate with the server.

**Communication**

Address

Port

Accessed By ☒ All CounterACT Devices (Recommended) ☐ Enterprise Manager

**Server Credentials**

Shared Secret

Verify Shared Secret

**Buttons:** Help Previous Next Finish Cancel

For a description of the Communication settings, see [Communication Settings](#).

Configure the following additional parameter in the *Server Credentials* section:

<b>Shared Secret / Verify Shared Secret</b>	The shared key is used to authenticate the RADIUS transaction. Enter the shared key as defined on the RADIUS server for transactions coming from this CounterACT Appliance.
---	---

### TACACS Server Settings

This section describes the details required when working with TACACS.

**Add Server - Step 2 of 4**

**Add Server**

✓ Name and Type  
 Settings  
 Test  
 Replicas

**Settings**  
 Define the TACACS server parameters. CounterACT will use these parameters to communicate with the server.

**Communication**

Address:

Port:

Accessed By: ☒ All CounterACT Devices (Recommended)  
☐ Enterprise Manager

**Server Credentials**

Shared Secret:

Verify Shared Secret:

Authentication Method: PAP

Help Previous Next Finish Cancel

For a description of the Communication settings, see [Communication Settings](#).

Configure the following additional parameters in the *Server Credentials* section:

<b>Shared Secret / Verify Shared Secret</b>	The shared key is used to authenticate the TACACS transaction. Enter the shared key as defined on the TACACS server for transactions coming from this CounterACT Appliance.
<b>Authentication Method</b>	<p>The method that the Forescout platform uses for user authentication against the TACACS server. The list is in ascending order of security.</p> <ul style="list-style-type: none"> <li><b>ASCII</b>: User passwords are transmitted in plain text; compatible with older TACACS versions.</li> <li><b>PAP</b> (Password Authentication Protocol): User passwords are encrypted symmetrically with the TACACS shared secret and transmitted.</li> <li><b>CHAP</b> (Challenge Handshake Authentication Protocol): Challenge-response method; plain-text user passwords are needed by both the Forescout platform and the TACACS server, but they are not transmitted.</li> <li><b>ARAP</b> (AppleTalk Remote Access Protocol): Apple implementation of CHAP.</li> <li><b>MS-CHAP</b> (Microsoft CHAP): More secure version of CHAP; plain text user passwords are not needed by the Forescout platform or the TACACS server.</li> </ul>

## Configure Server Tests

Define the parameters for testing the connection between a server and the User Directory Plugin. The Directory Server Test verifies that information can be resolved for the user name entered. The Authentication Server Test verifies user authentication using the credentials provided.

There is no Directory test for RADIUS and TACACS servers.

For Microsoft Active Directory servers, the fields in the Authentication section are populated with the Administrator information entered in the Settings pane.

**Add Server - Step 3 of 4**

**Add Server**

- ✓ Name and Type
- ✓ Settings
- Test**
- Replicas

**Test**

Define parameters to be used when testing the connection between the User Directory Plugin and the server. The Directory Server Test verifies that identity details can be resolved for a user. The Authentication Server Test verifies that user credentials can be authenticated.

**Directory Server Test Parameter**

User:

**Authentication Server Test Parameters**

User:

Password:

Verify Password:

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

Configure the following settings in this pane:

<b>Directory</b>	<b>User:</b> A user name to query. This should be a valid user in the domain.
<b>Authentication</b>	<b>User and Password:</b> Valid login credentials for testing if authentication works.

## Configure Replicas

Specify the organizational replica servers to be used as backup servers if the User Directory server defined in the *Name and Type* pane fails. This configuration is optional.

For details about how replica servers are used for Microsoft Active Directory, see [DNS Detection for Microsoft Active Directory](#).

**Add Server - Step 4 of 4**

**Add Server**

- ✓ Name and Type
- ✓ Settings
- ✓ Test
- Replicas

**Replicas**

Optionally define organizational replica servers to be used as backups if this server fails. Replicas are not used when 'DNS Detection' is selected in the Settings tab.

Search

IP Address	Name	Accessed By
No items to display		

**Add**  
**Edit**  
**Remove**

**Help** **Previous** **Next** **Finish** **Cancel**

### To add a replica server:

1. In the *Replicas* pane of the *Server* wizard, select **Add**.

**Add Replica Server**

Server Name

IP Address

Accessed By

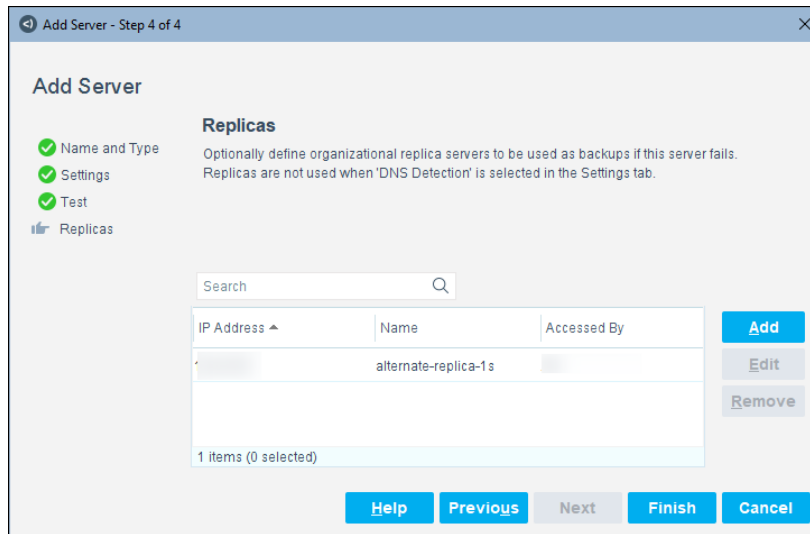
☒ All

☐ Enterprise Manager

**OK** **Cancel**

2. In the *Server Name* field, enter the replica server name.
3. In the *IP Address* field, enter the remote address of the replica server, such as an IP address, an FQDN address string, or an IPv6 address string.
4. Indicate whether an Appliance or Enterprise Manager can access the replica server, or select both to allow both device types to access the server.

5. Select **OK**. The server is added to the *Replicas* pane.



6. Select **Finish**. The configuration appears in the *User Directory* pane.

## Advanced Settings Configuration Tab

Advanced settings can be configured for a User Directory server only after the server is added to the User Directory Plugin. These settings cannot be defined in the Add Server wizard.

Advanced settings are not available for RADIUS and TACACS server types.

Use Advanced settings to:

- Copy non-default values from the server to the plugin.
- Reduce the number of unwarranted authentication failures in scenarios where there are several groups and domains.
- Optimize the way group information is retrieved.
- When TLS is used, define if Forescout platform presents a client certificate and if it verifies the user directory server certificate.

### To define advanced settings for a server:

1. Complete the User Directory Plugin configuration for the server.
2. Select the configuration from the *User Directory* pane.
3. Select **Edit**. The *Edit Server* dialog box opens.

#### 4. Select the **Advanced** tab.

**Edit Server**

Name and Type   Settings   Test   Replicas   **Advanced**

**Advanced**

Advanced settings can only be defined after the server configuration has been added.  
Use these settings to copy non-default values from the server to the plugin, reduce the number of unwarranted authentication failures, optimize how CounterACT retrieves group information, and define certificate presentation and verification behavior.

User Filter

Query Size

☐ Search and Bind

☒ Targeted Group Resolution

DNS Detection Refresh Interval (seconds)

**Certificate Settings for TLS**

☐ Present CounterACT client certificate

☒ Verify user directory server certificate

☐ Check user directory certificate revocation status using:

☐ CRL

☐ OCSP ☐ Soft-fail OCSP Requests

[Help](#) [OK](#) [Cancel](#)

#### 5. Define the following settings:

<b>User Filter</b>	<p>This attribute is used to identify users. For multiple attributes, separate each string with a comma. If the field is empty, the following defaults are used:</p> <ul style="list-style-type: none"> <li>For Microsoft Active Directory – sAMAccountName</li> <li>For Novell eDirectory – cn or uid</li> <li>For Oracle Directory – uid</li> <li>For IBM Lotus Notes – cn or uid</li> <li>For OpenLDAP Server – cn or uid</li> </ul>
<b>Query Size</b>	<p>This setting applies to Microsoft Active Directory servers only.</p> <p>This setting defines the maximum number of queries sent to the server simultaneously. Decrease this value if you encounter Size Limit server errors. The default setting is 1000.</p>



<b>Search and Bind</b>	<p>This setting does not apply to Microsoft Active Directory servers.</p> <p>If your User Directory Plugin test results indicate that authentication failed, this setting may resolve the problem.</p> <p>In environments with multiple groups and domains, a Bind DN pattern might not produce a unique DN for each user, and user authentication cannot proceed.</p> <p>When this option is selected, the User Directory Plugin ignores the Bind DN pattern, and:</p> <ol style="list-style-type: none"> <li>1. Binds to the directory with the user credentials entered in the Administrator Bind DN field in the Settings tab.</li> <li>2. Searches the directory for a user with the same name as the authentication request's username field.</li> <li>3. Retrieves the user's unique DN from the directory.</li> <li>4. Binds with the DN and the authentication request's Password field.</li> </ol>
<b>Targeted Group Resolution</b>	<p>This setting applies to Microsoft Active Directory servers only.</p> <p>When this option is selected, Forescout platform optimizes the way it retrieves group information. Use this option to reduce traffic in large-scale network environments with complex group hierarchies. Instead of the default method of retrieving a full listing of groups at regular intervals, this setting instructs the plugin to store primary group IDs and then selectively query for further group information.</p> <p>For newly added servers, this setting is enabled by default.</p> <p><b>Note:</b> For Microsoft Active Directory servers, you cannot enable both the <i>Targeted Group Resolution</i> option here and the <i>Include parent groups</i> setting in the Name and Type tab.</p>
<b>DNS Detection Refresh Interval</b>	<p>This setting applies to Microsoft Active Directory servers for which <i>DNS Detection</i> was selected in the Settings tab. See <a href="#">DNS Detection for Microsoft Active Directory</a>.</p> <p>This setting defines the frequency, in seconds, at which the plugin queries domain controller addresses.</p>

<b>Certificate Settings for TLS</b>	<p>These settings define how certificates are used and verified between Forescout platform and the server. These settings apply only when TLS is used to encrypt communication with the User Directory server. See <a href="#">Use TLS</a> in the Settings tab.</p> <p>For detailed information about defining and provisioning certificates, refer to the Forescout Administration Guide section that describes how to configure the certificate interface.</p>
<b>Present CounterACT client certificate</b>	<p>When this option is selected, Forescout platform presents a client certificate to the user directory server.</p>
<b>Verify user directory server certificate</b>	<p>When this option is selected, Forescout platform verifies the user directory server certificate.</p>
<b>Check user directory certificate revocation status using</b>	<p>When this option is selected, Forescout platform checks that the user directory server certificate has not been revoked.</p> <ul style="list-style-type: none"><li>▪ <b>CRL:</b> Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority.</li><li>▪ <b>OCSP:</b> Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status.<ul style="list-style-type: none"><li>- <b>Soft-fail OCSP Requests:</b> If Forescout platform does not receive a response from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.</li></ul></li></ul>

## Duplicate Servers

Typically, there are several User Directory servers in a network environment. You can repeat the [Configuration](#) procedures to manually define additional servers or you can duplicate an existing server profile and edit its properties as required. Using an existing server profile as the basis for a new server configuration eliminates the need to define each of the server settings from scratch.

### To duplicate a server:

1. Select the existing server in the *User Directory* pane and select **Duplicate**.
2. The *Edit Server* wizard opens. Most fields are populated with the settings of the existing server.
3. Modify the server settings to create a new server definition.

 You must supply a unique address to differentiate this server.

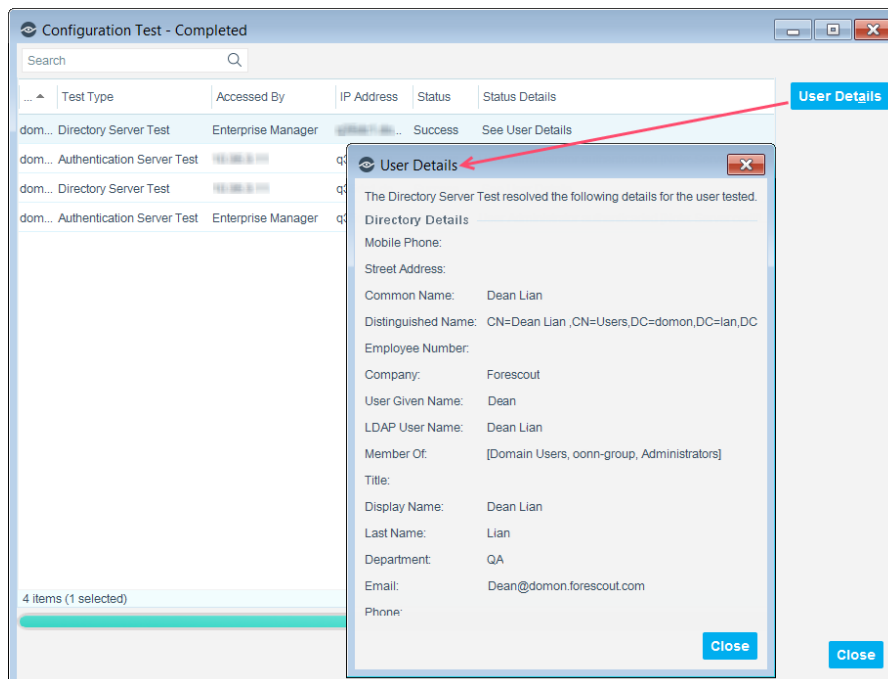
4. Select **OK**. The new server definition appears in the *User Directory* pane.

## Test the Configuration

To ensure that the plugin can connect to a server, it is recommended to run a test using the settings defined in [Configure Server Tests](#).

### To test a server configuration:

1. Select the server in the *User Directory* pane and select **Test**. A configuration test runs for each CounterACT device selected in the *Accessed By* field.
2. To see the results of a Directory test, select the row and select **User Details**.



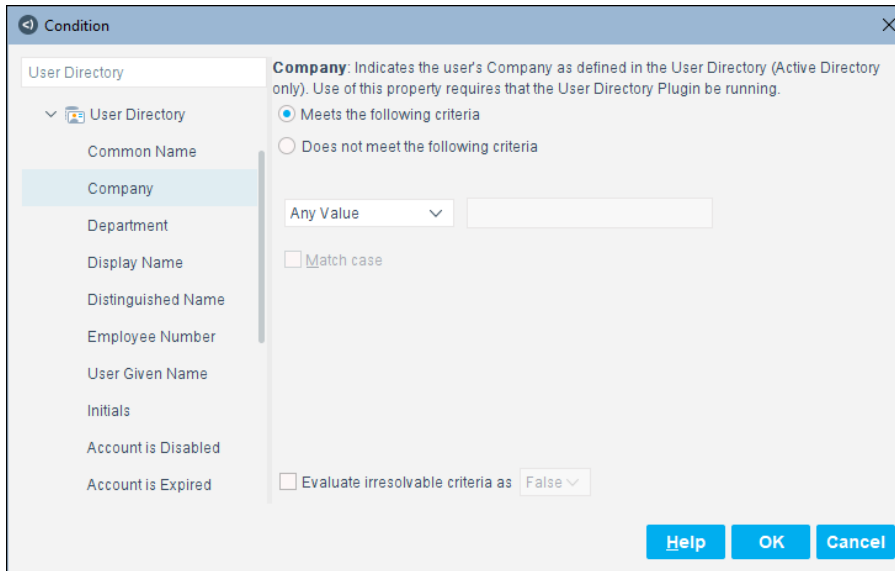
## Working with Policies

Use policy tools to detect endpoints with specific User Directory attributes. For example, create a policy that detects endpoint users in a specific Active Directory department or with a specific distinguished name.

### Detect Endpoints with User Directory Attributes

You can use a policy to detect the following User Directory attributes on endpoints:

- *Account is Disabled* (Active Directory only)
- *Account is Expired* (Active Directory only)
- *Common Name*
- *Company* (Active Directory only)
- *Department* (Active Directory only)
- *Display Name* (Active Directory only)
- *Distinguished Name*
- *Email*
- *Employee Number* (Oracle Directory only)
- *Initials*
- *Last Name*
- *LDAP User Name*
- *Member Of*
- *Mobile Phone*
- *Password Last Set*
- *Phone*
- *Street Address*
- *Title* (Active Directory only)
- *User Given Name*



Refer to the *ForeScout Administration Guide* for details about working with policies. See [Additional ForeScout Documentation](#) for information on how to access the guide.

## Display User Directory Information at the Console

Information learned by the User Directory Plugin can be viewed in the Console:

- In the *Detections* pane
- In the *User* section of the *Profile* tab

The screenshot displays the CounterACT Enterprise Manager Console interface. The top navigation bar includes 'File', 'Reports', 'Actions', 'Tools', 'Log', 'Display', and 'Help'. The main header shows the 'FORESCOUT' logo and navigation links for 'Home', 'Asset Inventory', and 'Policy'. The left sidebar contains a 'Views' section with 'All Hosts (584)' selected, and a 'Filters' section with 'All' selected. The main content area shows a table of hosts under the 'All Hosts' view. Below the table, the 'Profile' tab is active, displaying the details for the user 'administrator'.

Host	IPv4 Address	Display Name	Department	Email	Phone	S...	...	...
DOM311Q...	...	Fay Lomain	IT	Lomain@scout.com	6009666	Do...	...	...
DOM321Q...	...	Dan Aclay	Lab	Aclay@scout.com	6009624	Do...	...	...
DOM321Q...	...	Raul Polly	Administration	Polly@scout.com	6009645	Do...	...	...

Below the table, the 'Profile' tab is active, showing the user 'administrator' with the following details:

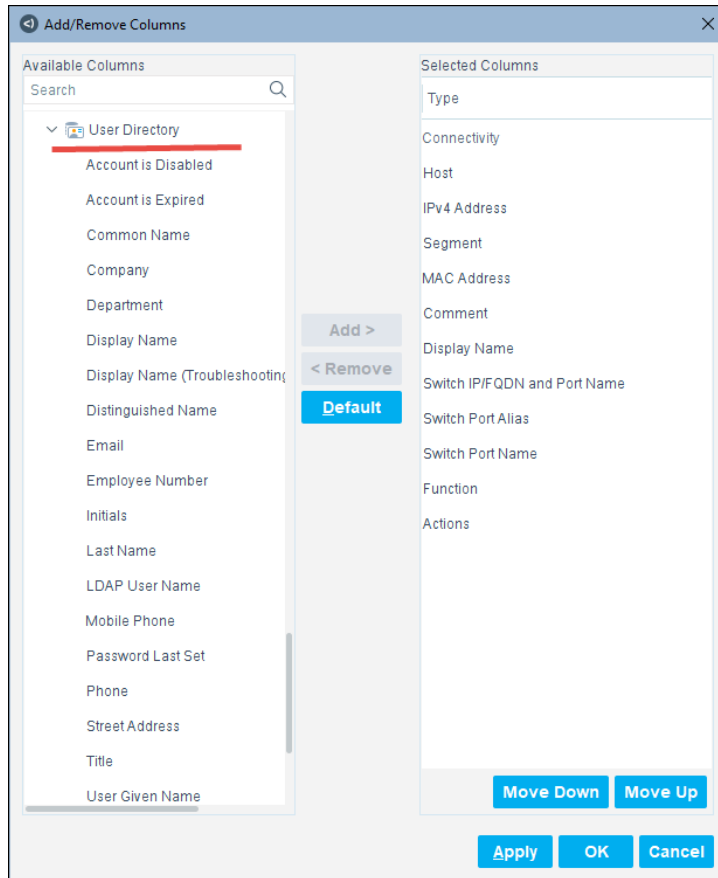
- User:** administrator **IPv4**
- Address:** QA-EAF61583C255 **Function:** Computer
- MAC Address:** 0050569F5028 **Domain:** DOM31 **Operating System:** Windows XP Professional

The 'User' profile is expanded, showing the following details:

- General:** Account is Disabled: No, Account is Expired: No, Company: Nons
- Security:** Department: IT, Display Name: Fay Lomain, Distinguished Name: Administrator, Email: Lomain@scout.com, Employee Number: 1, Initials: F.L., Last Name: Lomain, LDAP User Name: Administrator, Member Of: Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners
- More:** Mobile Phone: 6666666666, Password Last Set: 8/25/14 1:26:24 PM, Phone: 6009666, Street Address: 24 W Paul, Title: IT Admin

### To display/hide columns:

1. Right-click a table header in the *Detections* pane and select **Add/Remove Columns**.
2. Expand the *Properties* node and then expand the *User Directory* node.



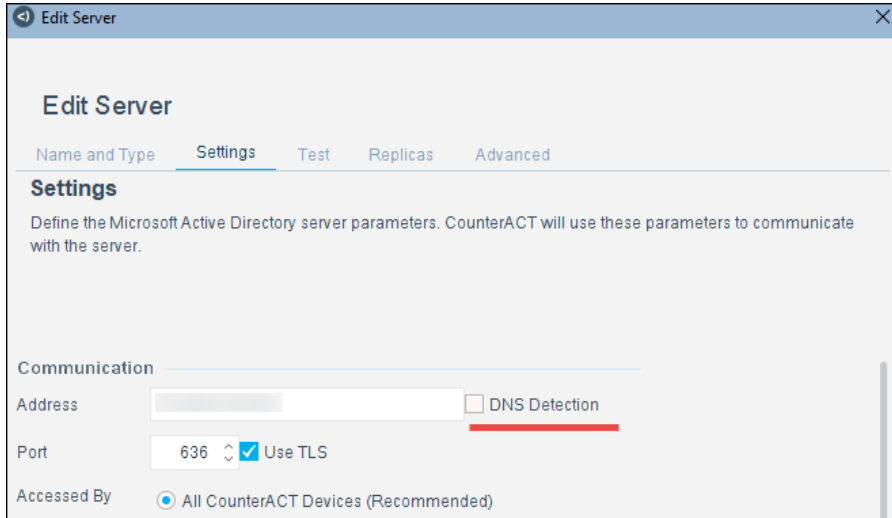
3. To add columns to the table:
  - a. In the *Available Columns* list, select one or more columns.
  - b. Select **Add**. The selected columns are moved to the *Selected Columns* list.
4. To remove columns from the table:
  - a. In the *Selected Columns* list, select the columns you do not want to display.
  - b. Select **Remove**. The selected columns are moved to *Available Columns* list.
5. (Optional) Use the *Move Down* and *Move Up* options to reorder the columns. The first column in the *Selected Columns* list is displayed in the leftmost position in the table.
6. Select **OK**.

## Additional Information

This section provides more detailed information about the plugin.

## DNS Detection for Microsoft Active Directory

The Microsoft Active Directory server configuration includes a *DNS Detection* option in the *Settings* tab.



### When DNS Detection Is Not Enabled

When the server is added, the User Directory Plugin constructs a list that includes:

- The server address configured in the Settings tab, Communication section
- All the server addresses configured in the Replicas tab


The address defined in the Settings tab is first in the list. There is no specific order among the replica servers.

For each CounterACT Appliance, the list is divided into two parts:

- The IP addresses of servers that are accessed by the evaluating Appliance ('accessed by me')
- The IP addresses of servers that are accessed by other Appliances ('accessed by others')

Forescout platform connects to the server as follows:

1. Forescout platform attempts to connect to the first reachable server in the 'accessed by me' list. If the list is empty, Forescout platform delegates the connection to one of the 'accessed by others' servers.
2. If a server is unreachable (service not available), Forescout platform attempts to connect to the next server in the same list.
3. If a server is reachable but a timeout (congested network or firewall configuration) exceeds the configured 10-second maximum timeout, Forescout platform attempts to connect to the next server in the same list.

 The timeout parameter is configurable per Appliance using the following command:  
`fstool ad set_property config.timeout.value <new timeout sec>`



## When DNS Detection Is Enabled

When *DNS Detection* is enabled, the user does not provide primary server or replica server IPs. Forescout platform automatically learns directory server addresses. This is recommended in network environments where several domain controllers function as replicas.


In DMZ environments, do not enable DNS Detection for CounterACT Appliances if the DNS server is not reachable from Appliances.

Forescout platform identifies the primary directory server as follows:

1. Using DNS lookup, the User Directory Plugin constructs a list of all potential directory servers.
2. Of the potential directory servers, the quickest to respond is selected as the primary server.
3. This primary server is used for each LDAP query.

If the primary server is unreachable (service not available) when it is evaluated, the plugin follows the procedure to identify a new primary directory server. By default, the primary server is evaluated hourly. See [DNS Detection Refresh Interval](#).

If the primary server is reachable but a timeout (congested network or firewall configuration) exceeds the configured 10-second maximum timeout, the plugin follows the procedure to identify a new primary directory server.

 *The timeout parameter is configurable per Appliance using the following command:*  
**`fstool ad set_property config.timeout.value <new timeout sec>`**

## Compatibility Across Servers

Endpoint properties in the user directories are shared with Forescout platform. The following table shows which properties are mapped from each directory type to Forescout platform.

Forescout Property Tag	MS Active Directory	Novell eDirectory	Oracle Directory	IBM Lotus Notes	OpenLDAP
<b>ad_cn</b>	cn	cn	cn	cn	cn
<b>ad_company</b>	company	company	company	company	company
<b>ad_department</b>	department	department	department	department	department
<b>ad_displayname</b>	displayname	displayname	displayname	displayname	displayname
<b>ad_employeenumber</b>	employeenumber	employeenumber	employeenumber	employeenumber	employeenumber
<b>ad_givenname</b>	givenname	givenname	givenname	givenname	givenname
<b>ad_initials</b>	initials				
<b>ad_isdisabled</b>	useraccountcontrol				

Fore Scout Property Tag	MS Active Directory	Novell eDirectory	Oracle Directory	IBM Lotus Notes	OpenLDAP
<b>ad_isexpired</b>	accountexpires				
<b>ad_lm_fld1</b>					lmPassword
<b>ad_lm_fld2</b>					sambaLmPassword
<b>ad_mail</b>	mail	mail	mail	mail	mail
<b>ad_memberof</b>	memberof	groupMembership	memberof	groupMembership	member
<b>ad_mobile</b>	mobile	mobile	mobile	mobile	mobile
<b>ad_name</b>	name	cn	name	cn	cn
<b>ad_nt_fld1</b>					ntPassword
<b>ad_nt_fld2</b>					sambaNtPassword
<b>ad_pwd_fld</b>					userPassword
<b>ad_pwdlastset</b>	pwdlastset				
<b>ad_sn</b>	sn	sn	sn	sn	sn
<b>ad_streetaddress</b>				officestreetaddress	street
<b>ad_telephone number</b>	telephonenumber	telephonenumber	telephonenumber	telephonenumber	telephonenumber
<b>ad_title</b>	title	title	title	title	title
<b>object_sid</b>	objectSid				
<b>primary_group_id</b>	primaryGroupID				

## Chapter 2: Corporate and Guest Management

### Corporate and Guest Control

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, see [Chapter 1: User Directory Management](#).
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

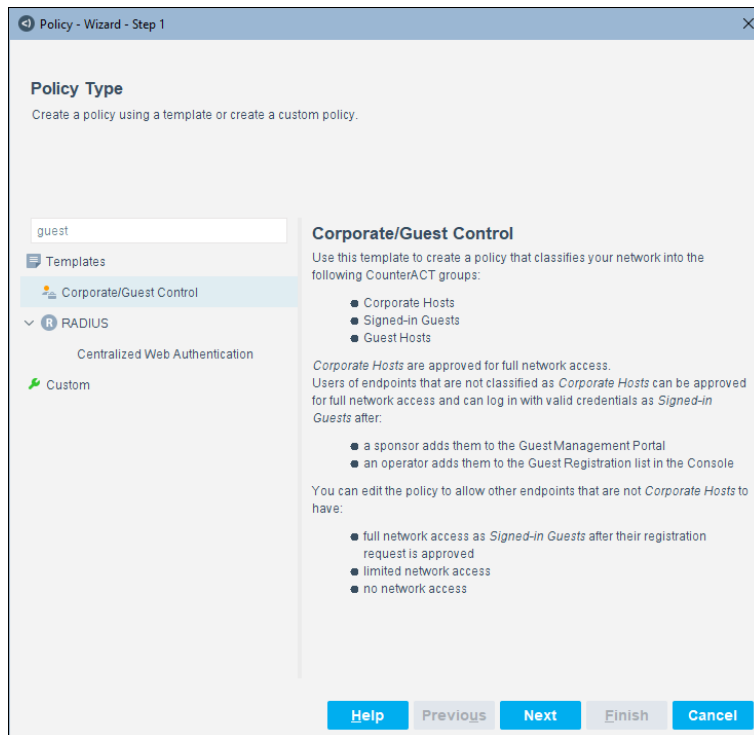
Deploy a policy created by the Corporate/Guest Control policy template to classify your network into Corporate Hosts, Signed-in Guests and Guest Hosts groups, and to deploy options for handling guests.

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:**

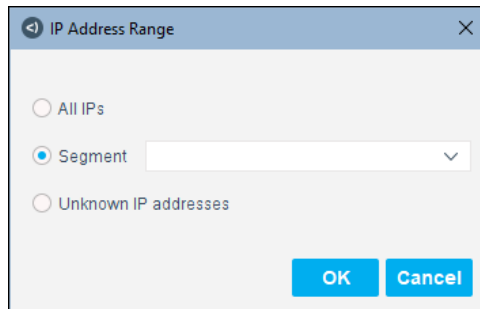
1. Select **Add** from the Policy Manager.
2. Select **Corporate/Guest Control**.




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**).
  4. Select **Next**. The *Guests* page opens.



## 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](#)

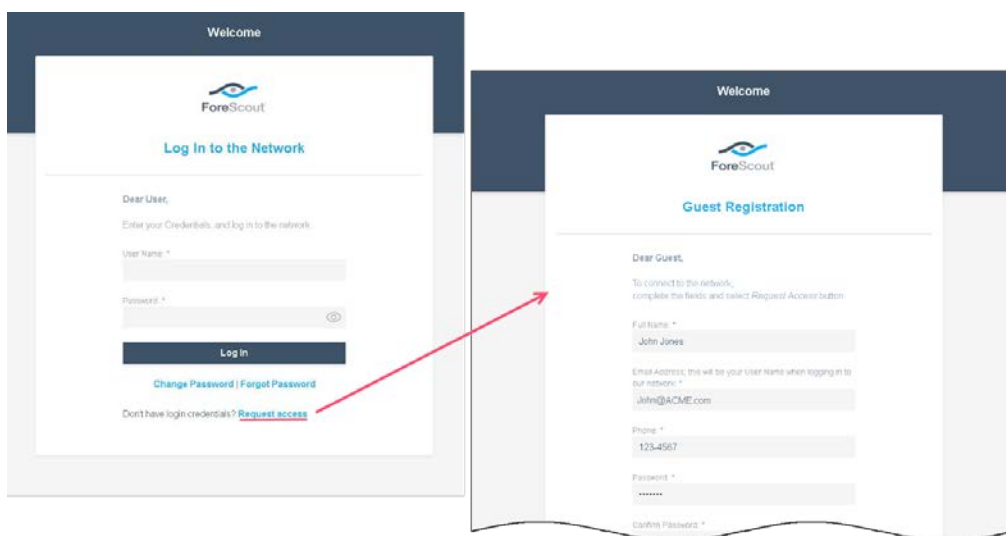


- [Assign to VLAN](#)
- [Virtual Firewall](#)

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.

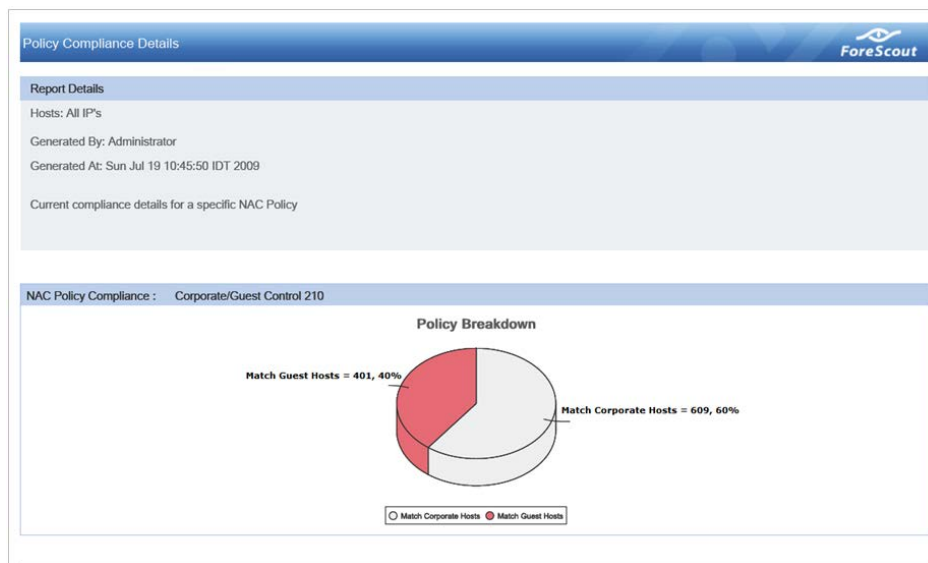
 *The Reports tool provides tools to customize reports and schedule automatic report generation. For more information about the Reports tool, see the Forescout Console User Guide.*

### **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 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. See [Guest Management Pane](#).

### 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.

Guest Management Task	Sponsors Using Guest Management Portal	Operators Using Guest Registration Pane
View guests.	✓	✓
Add pre-approved guests, and include the following information: <ul style="list-style-type: none"> <li>▪ Full name</li> <li>▪ Email (Required)</li> <li>▪ Phone number</li> <li>▪ Comment</li> </ul>	✓	✓
Include the following additional guest information when adding or approving guests: <ul style="list-style-type: none"> <li>▪ Date range of network access approval (Required)</li> <li>▪ Tags</li> <li>▪ Message to be sent to the guest</li> <li>▪ Company name</li> <li>▪ Location</li> <li>▪ Comment</li> </ul>	✓	
Include the following additional guest information when adding or approving guests: <ul style="list-style-type: none"> <li>▪ Password for network access.</li> </ul>		✓
Create tags to be assigned to guests.		✓
Approve network access for guests who submitted a Guest Registration form.	✓	
Decline network access for guests who submitted a Guest Registration form.	✓	
Revoke guests who were approved for network access.	✓	

Guest Management Task	Sponsors Using Guest Management Portal	Operators Using Guest Registration Pane
Remove guests from the Console and the Guest Management Portal guest lists.		✓
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.		✓

## Guest Management Portal

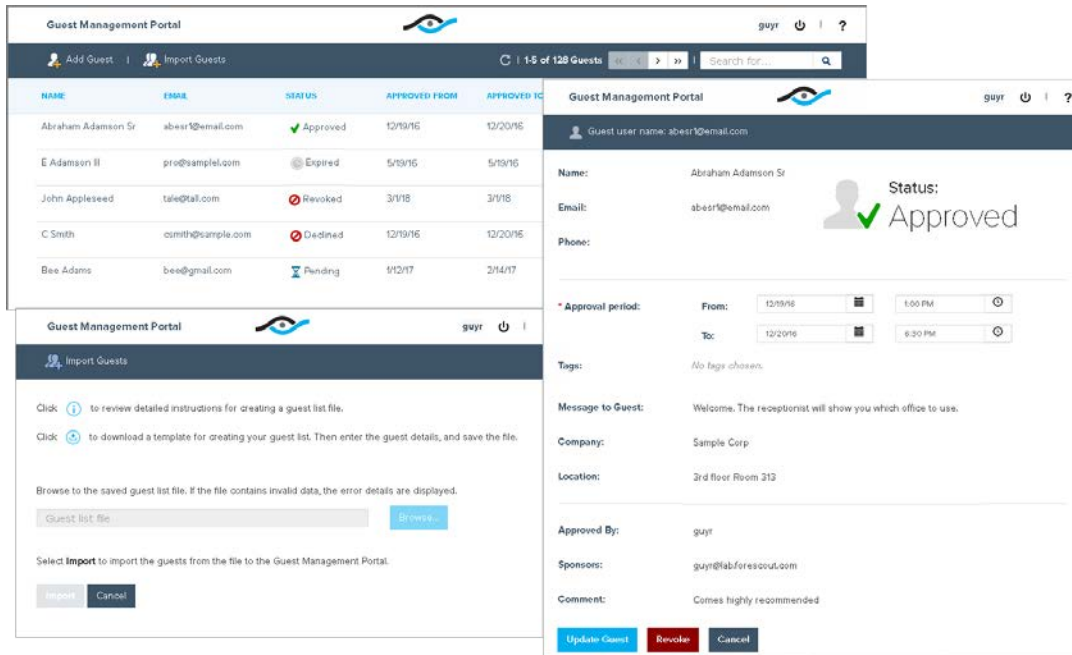
The Guest Management Portal is a Web-based portal that enables corporate personnel to view and manage network guests who have requested access to the organization's network. When access is approved, guests can browse the network and possibly use other network resources.


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, or they will not be able to 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

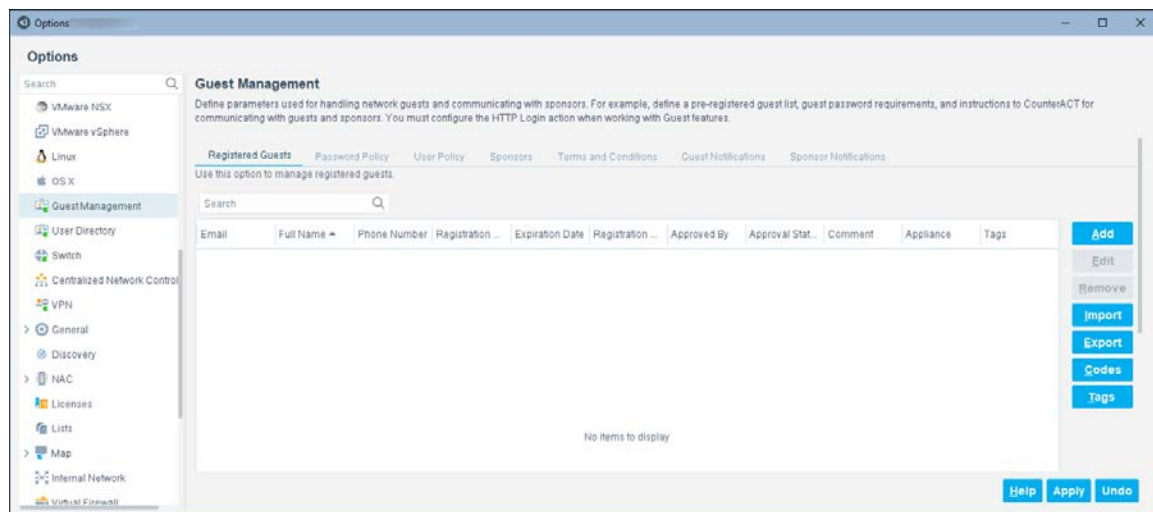
In the *Guest Management, Registered Guests* tab, Forescout operators can perform the following guest management activities.

- Add approved guests, edit and remove them:
  - [Adding Guests](#)
  - [Removing Guests](#)
  - [Purging Inactive Guests](#)
  - [Editing Guests](#)
- 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.

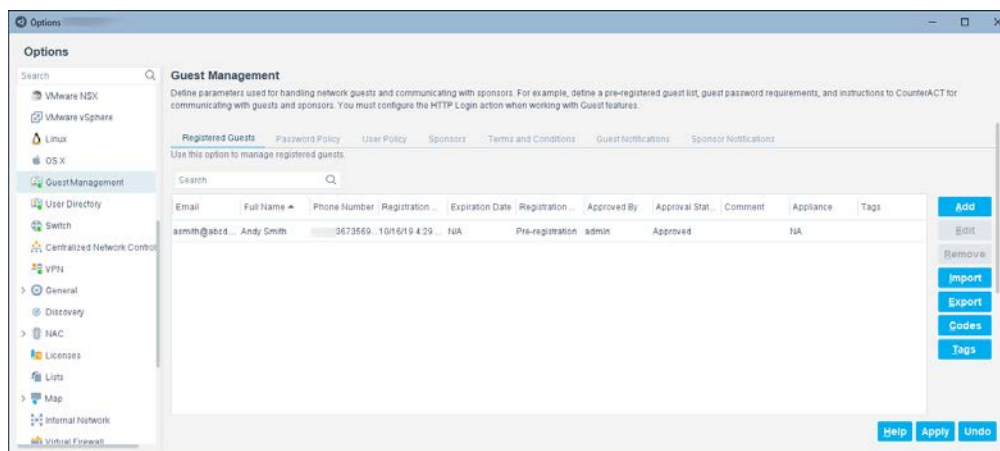
### Adding Guests

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

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

A screenshot of the 'Add Guest' dialog box. It contains several input fields: 'Email Address', 'Full Name', 'Password', 'Verify Password', 'Phone Number', and 'Comment'. At the bottom right are 'OK' and 'Cancel' buttons.

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:

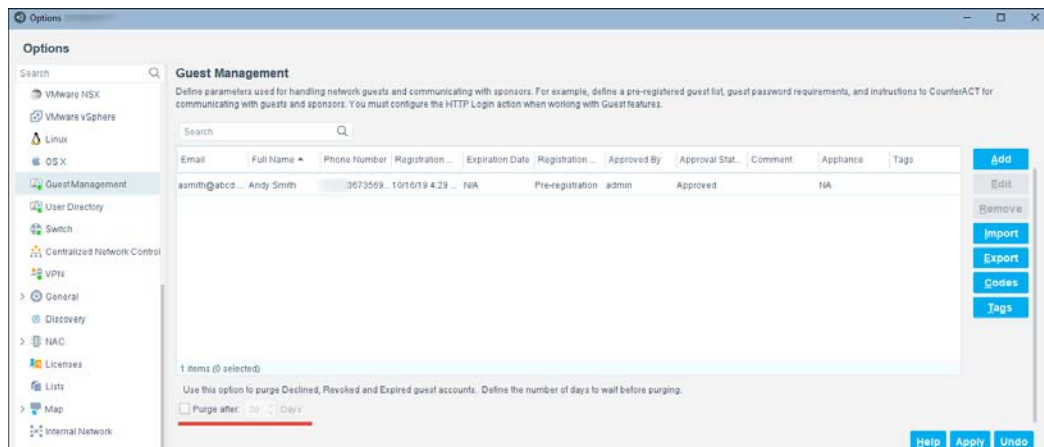
1. In the *Registered Guests* tab of the *Guest Management* pane, select a guest entry.
2. Select **Remove** and then select **Apply**.

## 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.



**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:

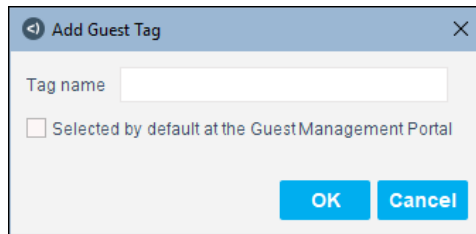
1. In the *Registered Guests* tab of the *Guest Management* pane, select **Tags**.

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.

3. Select **Add**. The *Add Guest Tag* dialog box opens.

A screenshot of the 'Add Guest Tag' dialog box. It has a title bar with a back arrow, 'Add Guest Tag', and a close button. Inside, there is a text input field labeled 'Tag name'. Below it is a checkbox labeled 'Selected by default at the Guest Management Portal'. At the bottom right are 'OK' and 'Cancel' buttons.

**Add Guest 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.

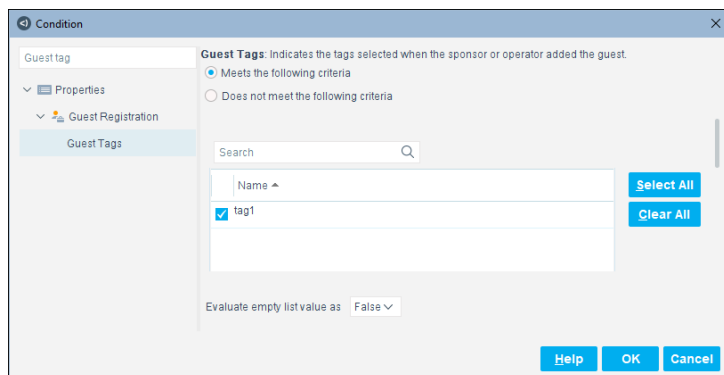
#### *Create Policies with Your Tags*

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

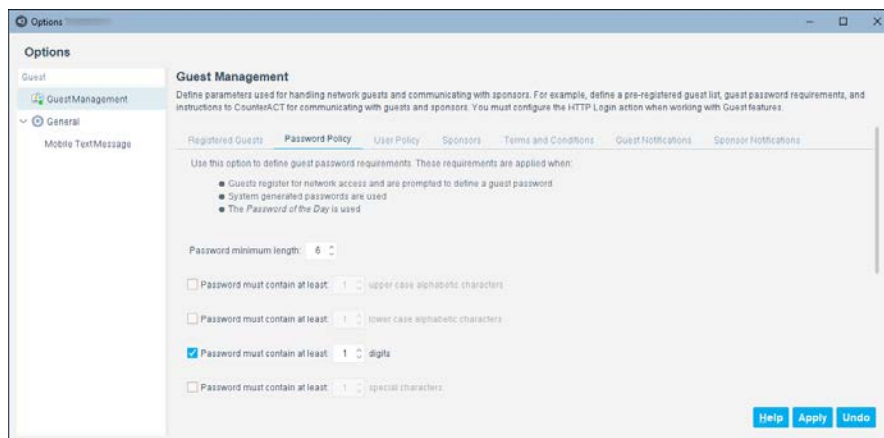
In the Guest Management pane, use the *Password Policy* tab to configure requirements, such as minimum length or special character requirements, for passwords used by approved guests to log in to the network. These requirements are applied to:

- 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:

1. Select the **Password Policy** tab of the *Guest Management* pane.



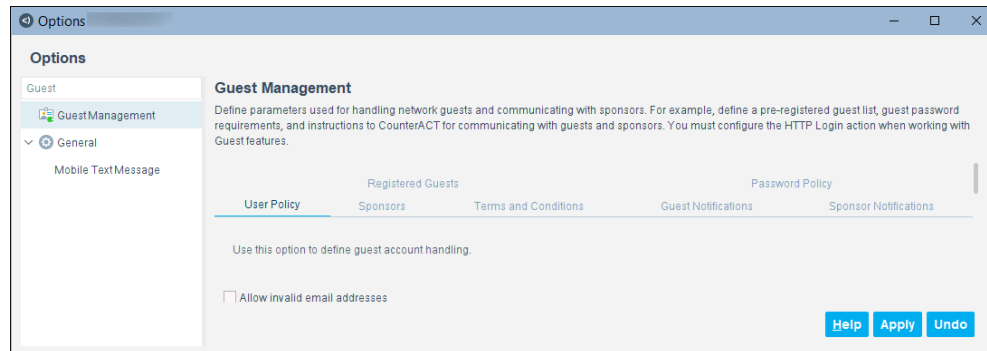
2. Define any of the following password requirements:
  - Minimum password length - the default, minimum length is 6 characters
  - Minimum number of uppercase characters to include
  - Minimum number of lowercase characters to include

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

3. Select **Apply** to save your changes in the configuration.

### 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.

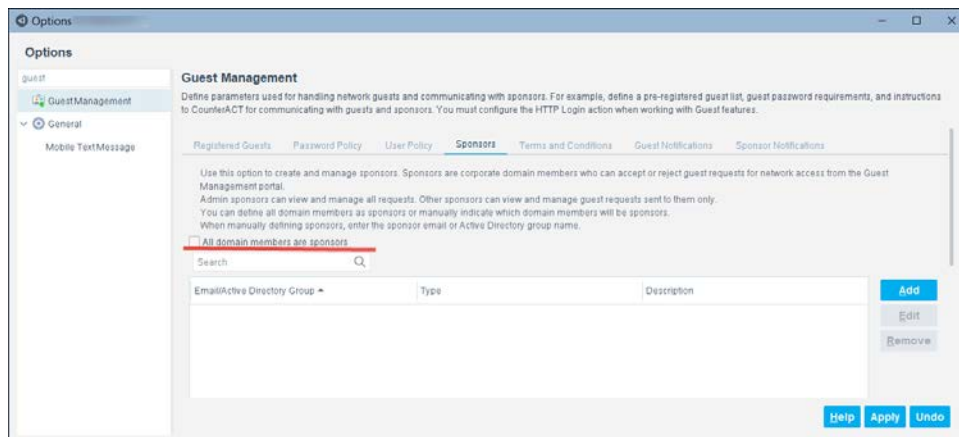
Add sponsors in any of the following ways:

- Globally, by selecting all user directory members
- Individually, by defining an email address

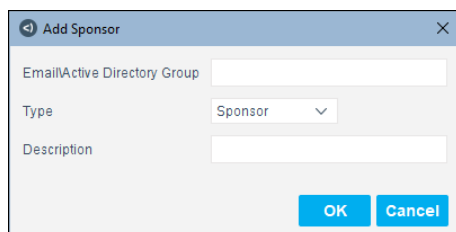
- By group, by defining an Active Directory group

### 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.



### Add Sponsor

- b. Define the following sponsor information:

<b>Email\Active Directory Group</b> (required)	Define either of the following: <ul style="list-style-type: none"> <li>▪ Enter the Active Directory email address of the individual you want to define as a sponsor.</li> <li>▪ Enter a corporate Active Directory group name to assign all its group members as sponsors.</li> </ul>
<b>Type</b> (required)	Select a sponsor type. <ul style="list-style-type: none"> <li>▪ <b>Sponsor</b> - can access the portal to view and manage only guests that are assigned to them.</li> <li>▪ <b>Admin Sponsor</b> - 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.</li> </ul>



<b>Description</b> (optional)	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.

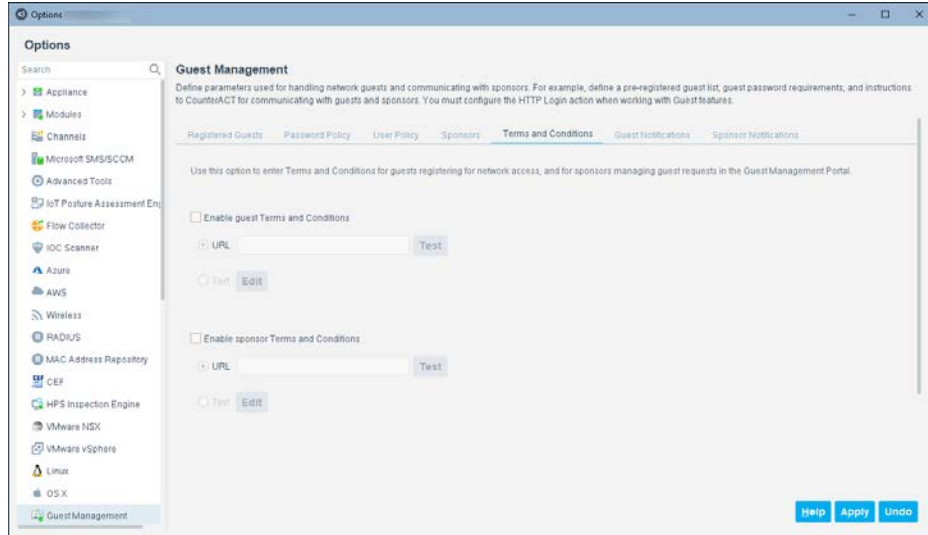
The screenshot shows the 'New Guest' form in the Guest Management Portal. The form has a dark header with the portal name and a user profile icon. The main form area is white with a dark sidebar on the left. The form fields are as follows:

- Name:** Text input field.
- \*Email:** Text input field.
- Phone:** Text input field with a country code dropdown (USA) and a phone number input (209 555-5555).
- \*Approval period:** Two rows of date and time pickers. The first row is for 'From' (5/23/16, 5:58 PM) and the second row is for 'To' (5/24/16, 11:59 PM).
- Tags:** Text input field with a placeholder 'Add a tag'.
- Message to Guest:** Text area with a placeholder 'Enter a message you want the guest to read'.
- Company:** Text input field with a placeholder 'Company name'.
- Location:** Text input field with a placeholder 'Location'.
- Comment:** Text input field with a placeholder 'Your comment about this guest'.

At the bottom of the form, there is a link: [By submitting this information, you accept the terms & conditions.](#) Below the link are two buttons: 'Approve' (blue) and 'Cancel' (grey).

### To configure terms and conditions:

1. Select the **Terms and Conditions** tab of the *Guest Management* pane.



## 2. Define the following:

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

## 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.

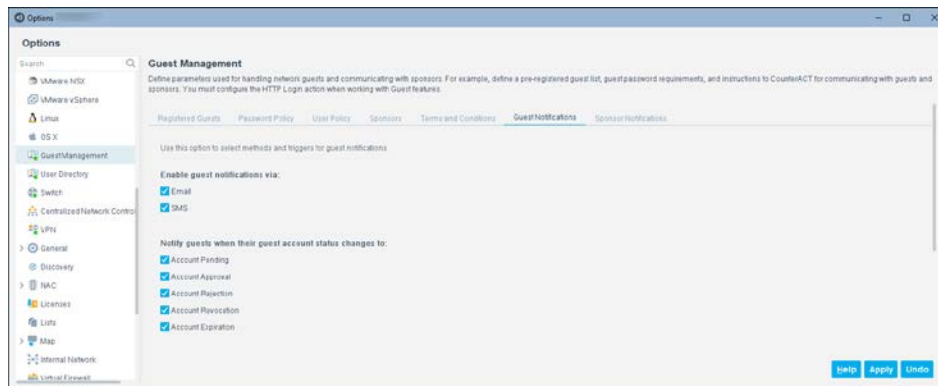
Email and phone information are provided:

- 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:

<b>Email</b>	Use email to deliver notifications to guests.
<b>SMS</b>	Use mobile text messaging (SMS) to deliver notifications to guests.

Notify guests when their guest account is set to:

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

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.

**Guest Management Portal**

guyr | ?

**New Guest**

Name: Ami

\* Email: ami@lab.com

Phone: (201) 123-4567

\* Approval period: From: 1/20/16 7:17 PM To: 1/28/16 11:59 PM

Tags: Add a tag

Message to Guest: Welcome to our company. Please enter through Building A.

Company: Sample Corporation

Location: Anytown

Comment: Comes highly recommended

By submitting this information, you accept the [terms & conditions](#).

**Approve** **Cancel**

**Network Access Approval**  
 CounterACT@App.com (CounterACT@App.com) (CounterACT@App.com) Add contact  
 To: ami@lab.com  
 Dear Ami  
 You have been approved for network access. Use the following credentials to log in:  
 Email: ami@lab.com  
 Password: io4vgp  
 Your account is approved:  
 From: 1/20/16 7:17 PM  
 To: 1/28/16 11:59 PM  
 Welcome to our company. Please enter through Building A.

**ForeScout**

**Network Access Request – John Jones**

John Jones is asking your approval to access the network as a guest

Full Name John Jones

Email giorat@t.com

Phone 123-4567

Requested Network Access Time Frame 01/22/2018 11:59 PM

Message to John Jones (Optional)  
 Please come by today. I'm looking forward to meeting you.

Guest Tags:

**Approve** **Decline**

**Network Access Approval**  
 CounterACT@App.com Add contact 22/01/2018 11:59  
 To: giorat@t.com  
 Dear John Jones,  
 You have been approved for network access. Use the following information to log in:  
 • Email: giorat@t.com  
 Your account is approved:  
 01/22/2018 11:59 PM  
 Please come by today. I'm looking forward to meeting you.

## Sponsor Notifications

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

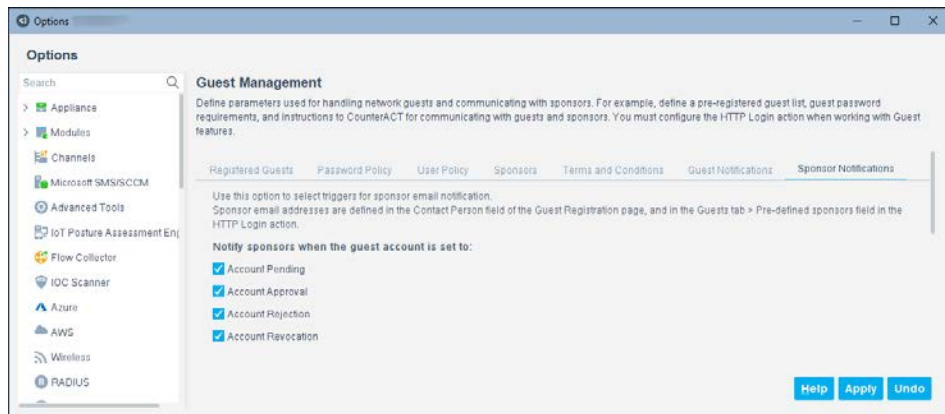
- The registering guest specifies the person's email address in the Contact Person Email field of the Guest Registration form.
- The person's email address is provided in the *Pre-defined sponsors for all guests* field in the Guests tab of the *HTTP Login* action.

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:

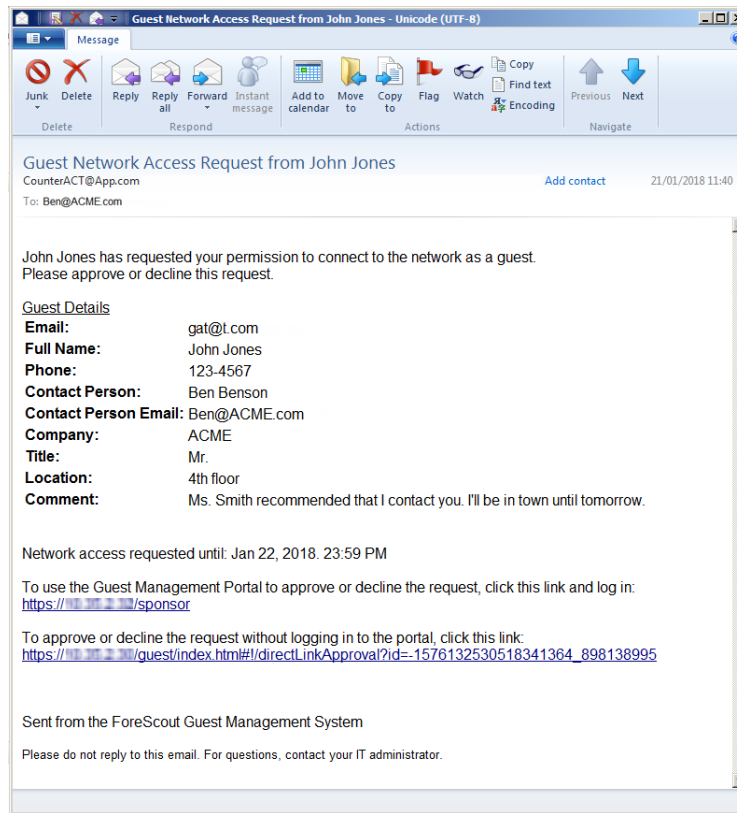
<b>Account Pending</b>	Notify the sponsors when a guest has requested network access.
<b>Account Approval</b>	Notify the sponsors when they approve a guest's network access request.
<b>Account Rejection</b>	Notify the sponsors when they decline a guest's network access request.
<b>Account Revocation</b>	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 new **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.

**Policy - Wizard - Step 4 of 5**

**Guests**

The settings in this pane define how to handle all endpoints that were not:

- classified as *Corporate Hosts*
- added by a sponsor to the Guest Management Portal
- added by an operator to the Guest Registration list in the Console

Note: By default, the HTTP Login action is disabled in the Guest Hosts sub-rule. Enable the action to apply **Sign In Guests**

Prompt unauthorized users with a Sign In page, where they can register as guests. After registration is confirmed and the user is signed in, the host is classified as a *Signed-In Guest*.

☒ **Show a Login page link where guests can register for full network access as Logged In Guests**

☒ Network access requests are automatically approved

☐ Guests must be approved by the sponsor they provide, or by:

Enter emails separated by commas

**Fine-tune Registration Options**

☐ Allow guests to skip login and have limited access only

**Buttons:** Help, Previous, Next, Finish, Cancel

- In the policy wizard **Guests** tab, ensure that the **Show a Login page link where guests can register for full network access as Logged In Guests** checkbox is selected.

**Policy - Wizard - Step 5 of 5**

**Sub-Rules**

Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

	Name	Conditions	Actions	Exce...
1	Corporate Host: Authentication Login: Login to an auth...			
2	Signed-in Gues ( Logged In Status: Logged In as a Gu...			
3	<b>Guest Hosts</b>	No Conditions		

**Buttons:** Add, Edit, Remove, Duplicate, Up, Down

**Buttons:** Help, Previous, Next, Finish, Cancel

- In the *Sub-Rules* tab, double-click the **Guest Hosts** sub-rule to open it for editing.

Policy: 'Corporate/Guest Control-d'--> Sub-Rule: 'Guest Hosts' -

---

**Name**

Name Guest Hosts Edit

Description None.

---

**Condition**

A host matches this rule if it meets the following condition:

All criteria are True ⚙️ 🔗

Criteria

No items to display

Add  
Edit  
Remove

---

**Actions**

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
<input checked="" type="checkbox"/>	HTTP Login	HTTP Login....
<input type="checkbox"/>	Virtual Firewall	Virtual Firew...
<input type="checkbox"/>	Assign to VLAN	Assign to VL...
<input checked="" type="checkbox"/>	Add to Group	Add to Grou...

Add  
Edit  
Remove

---

**Advanced**

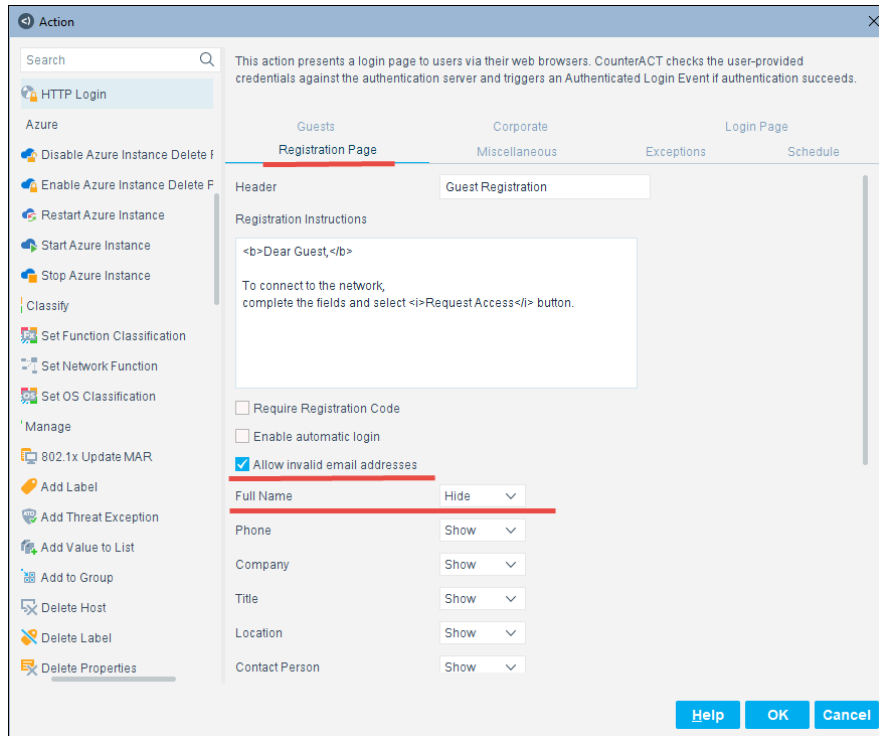
Recheck match Every 8 hours, All admissions Edit

Exceptions None.

Help OK Cancel

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.

Displayed	Type	Beginning of Description
Email	Label text	Captive Portal - Field label for: Email
Email Address; this will be your User Name when logging in to our network	Label text	Captive Portal - Field label for: Email (Guest Registration)
Enter your email address	Label text	Captive Portal - Field validation message for: 'Email' when is required
Enter your User Name (If you are a guest, enter your email address)	Label text	Captive Portal - Field validation message for: 'Username' when is required

Displayed	Type	Beginning of Description
Your User Name is your email address	Label text	Captive Portal - HTTP Login approve message

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:

Displayed	Type	Beginning of Description
Email	Label text	Guest Registration Email form field label

### 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.

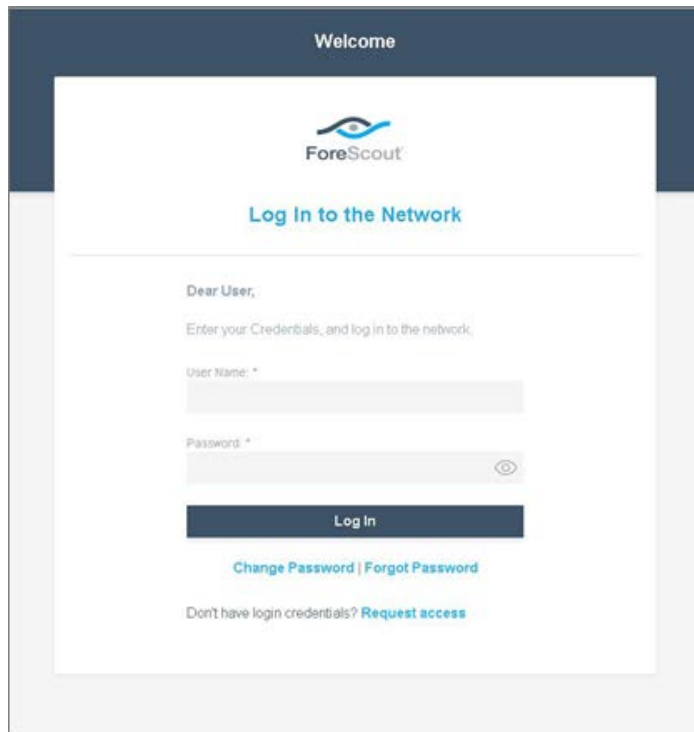
Displayed	Type	Beginning of Description
Each guest must have a unique email. {0} appears in lines {1}.	Error text	Error message for when guest list contains 2 or more guests with same...
Email	Label text	The Email label that appears in the Add Guest form
Email	Label text	The Email header that appears in the Guest Management Portal...
Email	Label text	Import Guests instructions text: step 2 Email column
Email address	Label text	Text that appears in New Guest page, Email field
Email address '{0}' has been added to the portal.	Label text	Approved success message
Enter an email address.	Error text	Empty email address is not allowed
Enter an email address.	Label text	Error displayed to user in New Guest page when the user did not enter...

Displayed	Type	Beginning of Description
The email address is too long. Enter up to 48 characters.	Label text	Guest form validation error when user entered an email with too much...
The guest at email address '{0}' has been updated.	Label text	Update success message
The portal already contains an Approved or Pending guest with email address...	Error text	Email address already exists. Can't override guest with status Approved...

## 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](#).

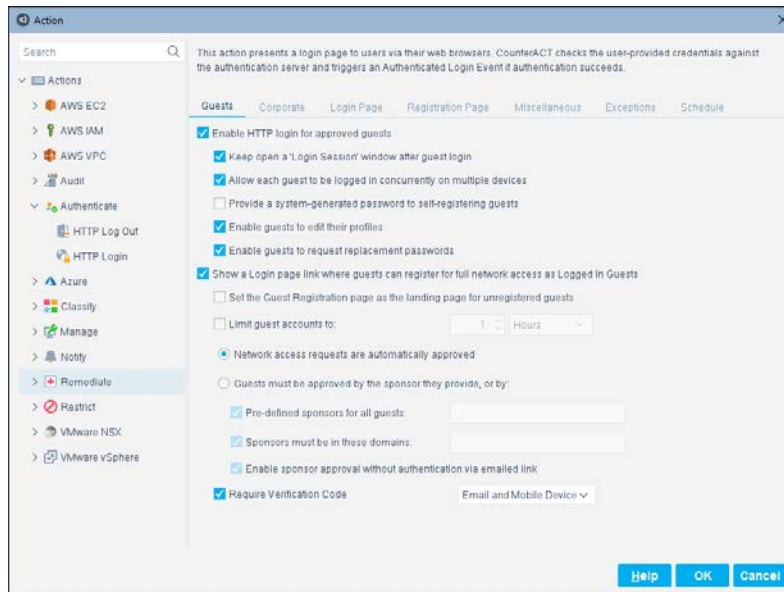
When the HTTP Login action is enabled, users attempting to access the network are redirected to a Login page where they must enter valid credentials. The user credentials are authenticated against the CounterACT Appliance.



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.

The image displays two side-by-side screenshots of the ForeScout web interface. The left screenshot shows the 'Log In to the Network' page. It features a 'Welcome' header, the ForeScout logo, and a 'Log In to the Network' title. Below this, there is a 'Dear User,' greeting, a prompt to 'Enter your Credentials, and log in to the network,' and input fields for 'User Name' and 'Password'. A 'Log In' button is present, along with links for 'Change Password' and 'Forgot Password'. At the bottom, a link for 'Don't have login credentials? Request access' is highlighted with a red underline. A red arrow points from this link to the right screenshot. The right screenshot shows the 'Guest Registration' form. It also has a 'Welcome' header and the ForeScout logo, with the title 'Guest Registration'. It includes a 'Dear Guest,' greeting and a prompt to 'To connect to the network, complete the fields and select Request Access button'. The form contains input fields for 'Full Name' (with 'John Jones' entered), 'Email Address' (with 'john@acme.com' entered), 'Phone' (with '123-4567' entered), 'Password', and 'Confirm Password'.

### 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:

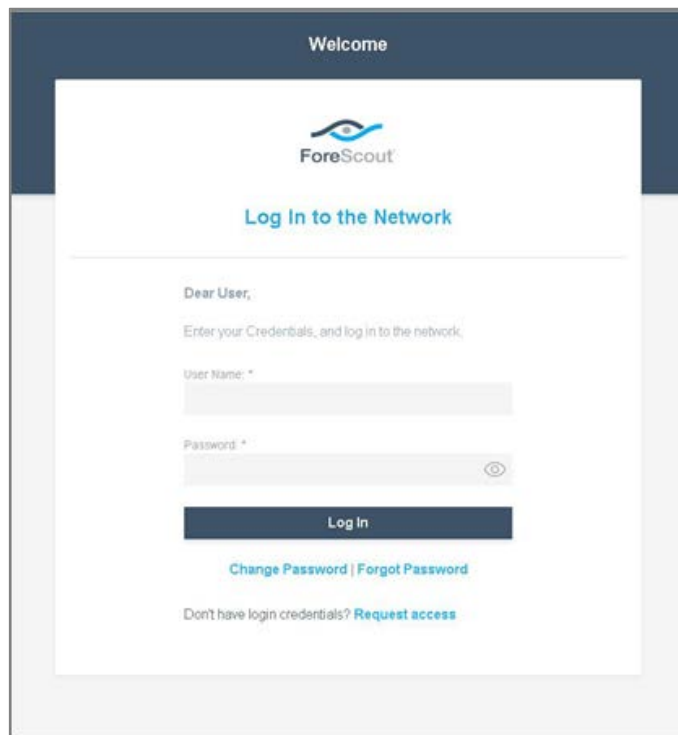
- [Corporate Tab](#): Defines which servers are used for authentication.
- [Login Page Tab](#): Defines the text that appears on the Login page.
- [Miscellaneous Tab](#): Defines addition configuration options such as encryption and compliance.

## HTTP Login Action Tabs

This section describes five of the HTTP Login action tabs.

### Login Page Tab

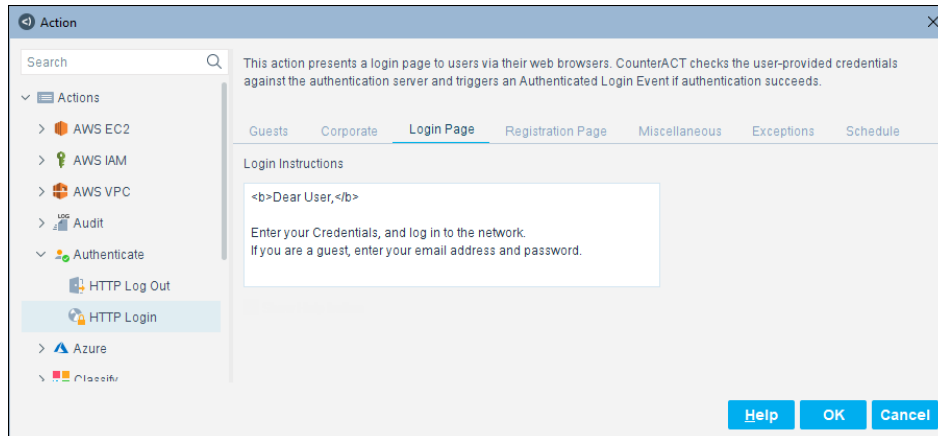
The *Login Page* tab is used to define what is displayed on the *Login* page. This page appears for both guest and corporate users.

A screenshot of a web-based login page for ForeScout. The page has a dark blue header with the word "Welcome" in white. Below the header is a white box containing the ForeScout logo (a stylized eye) and the text "Log In to the Network" in blue. Underneath, there is a "Dear User," greeting, followed by the instruction "Enter your Credentials, and log in to the network." There are two input fields: "User Name: \*" and "Password: \*". The password field has a toggle icon (an eye) to its right. Below the input fields is a dark blue "Log In" button. Under the button are two links: "Change Password" and "Forgot Password". At the bottom of the white box, there is a link that says "Don't have login credentials? Request access".

**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.

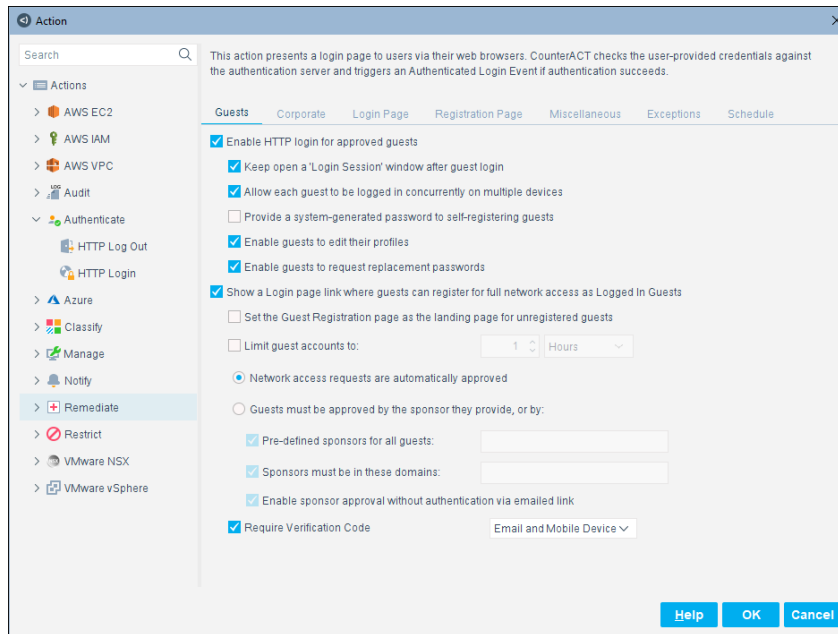
### ***Show Help Button***

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

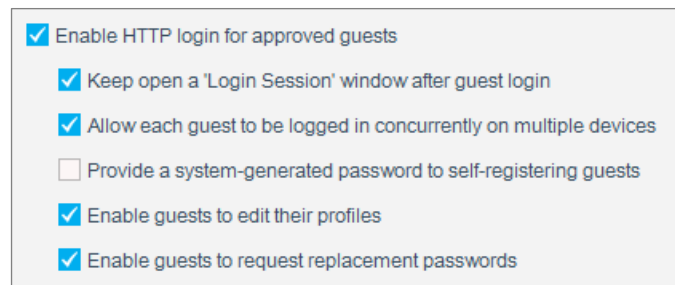
Use the *Guests* tab to define guest login session options, as well as a registration strategy.



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

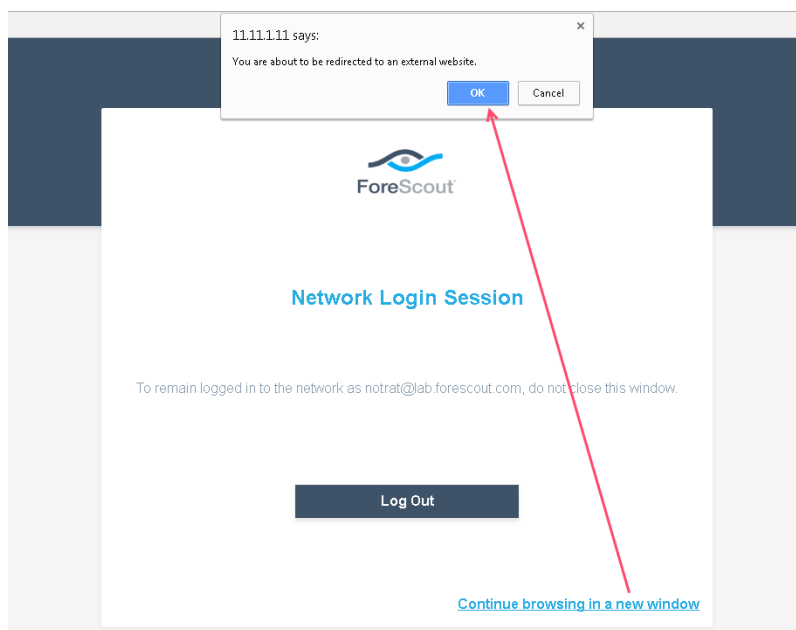
### Enable HTTP login for approved guests

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**.

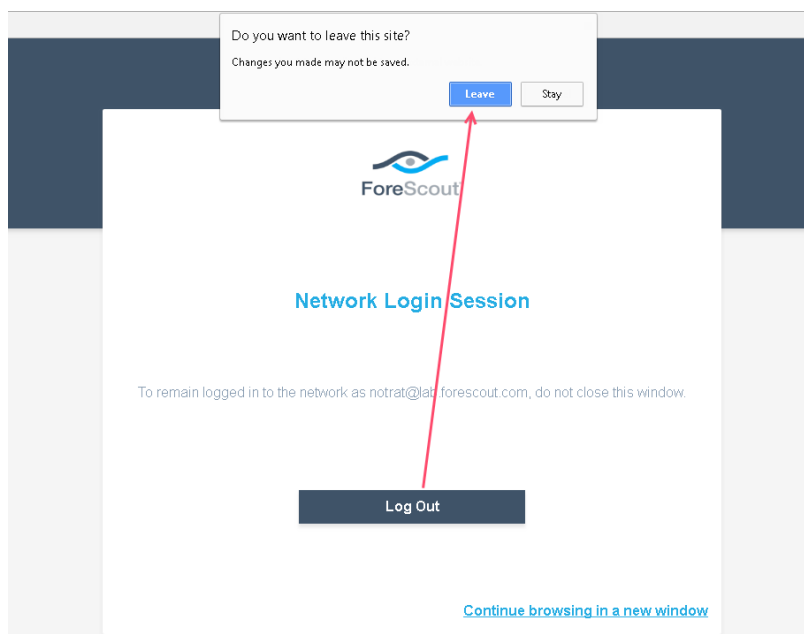




**Sample Corporate Login Session Window**

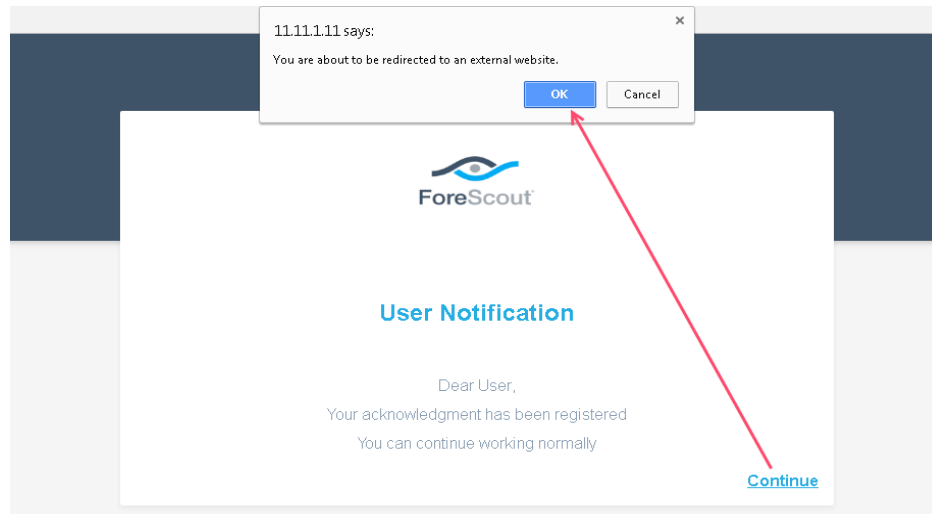
The user must keep the Login Session window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, ForeScout platform resolves the *Authentication, Signed In Status* property for the endpoint as *Signed In as a Guest*.

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***

☒ Show a Login page link where guests can register for full network access as Signed-in Guests

☐ Set the Guest Registration page as the landing page for unregistered guests

☐ Limit guest accounts to:

☒ Network access requests are automatically approved

☐ Guests must be approved by the sponsor they provide, or by:

☒ Pre-defined sponsors for all guests:

☒ Sponsors must be in these domains:

☒ Enable sponsor approval without authentication via emailed link

☒ Require Verification Code

### **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***

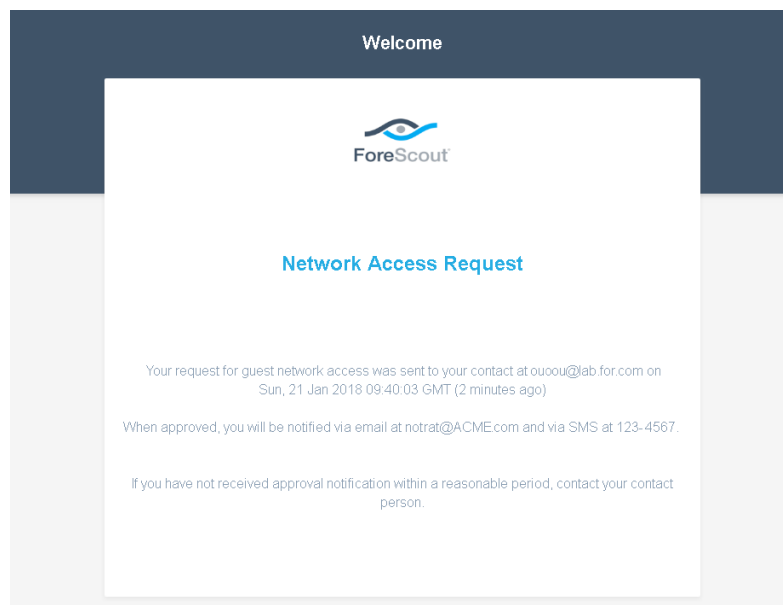
To automatically approve guests after submitting a Guest Registration form, select **Network access requests are automatically approved**. You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who is registered.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

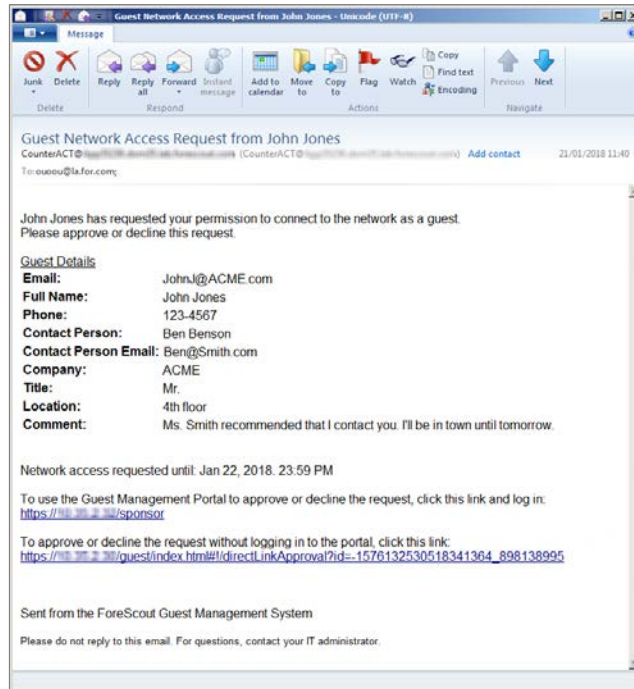
Before sponsor approval is completed, a notification page opens for the guest.



**Sample Guest Registration Request Pending Page**

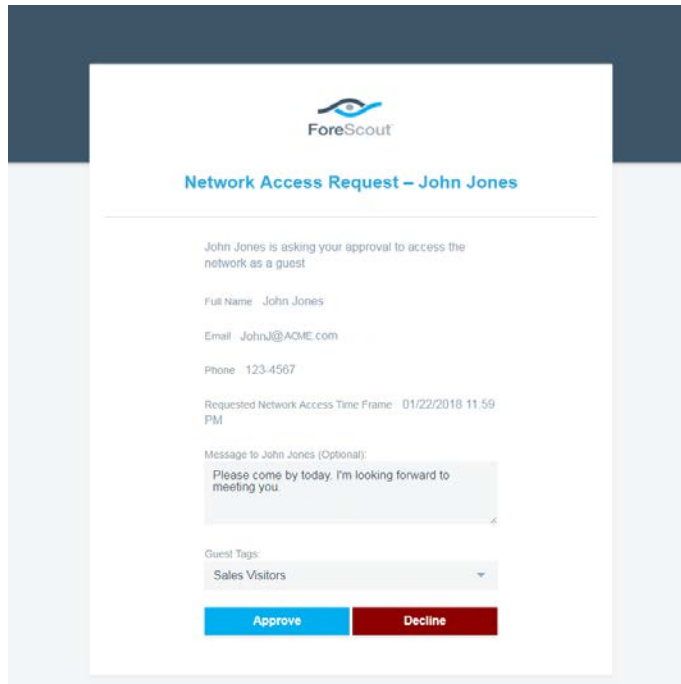
### ***Enable sponsor approval without authentication via emailed link***

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.



### **Sample Guest Registration Request Email**

- 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.



The image shows a web interface for a 'Network Access Request' by John Jones. At the top is the ForeScout logo. Below it, the title 'Network Access Request – John Jones' is displayed. The main content area contains the following information: 'John Jones is asking your approval to access the network as a guest', 'Full Name: John Jones', 'Email: JohnJ@ACME.com', 'Phone: 123-4567', and 'Requested Network Access Time Frame: 01/22/2018 11:59 PM'. There is a text box for a 'Message to John Jones (Optional):' with the text 'Please come by today. I'm looking forward to meeting you.' Below this is a 'Guest Tags' dropdown menu currently showing 'Sales Visitors'. At the bottom are two buttons: 'Approve' (blue) and 'Decline' (red).

### 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.

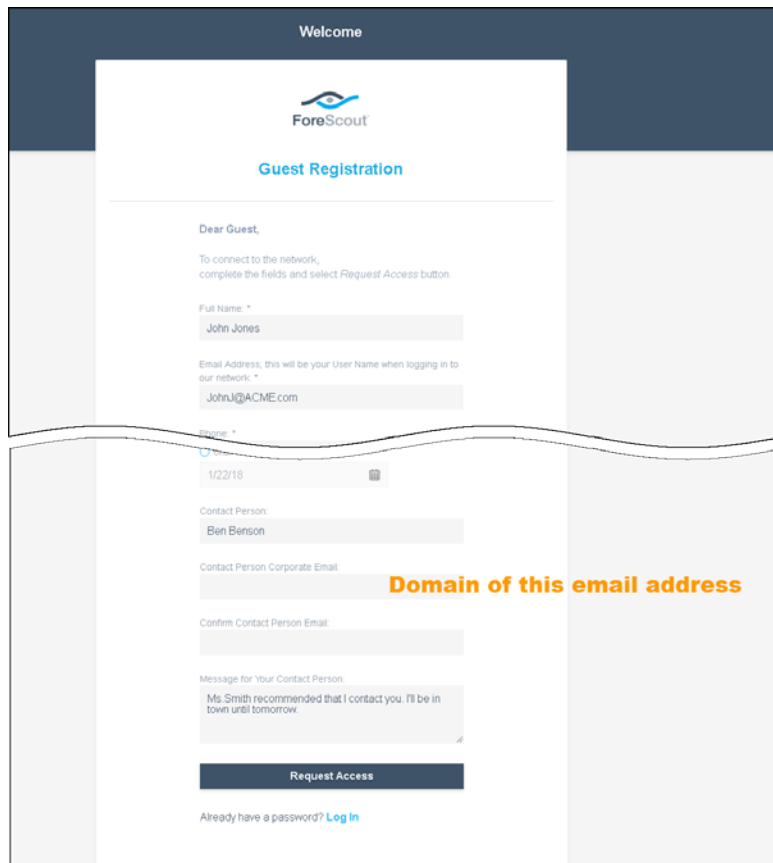
 If **Enable sponsor approval without authentication via emailed link** is selected, it is recommended to select **Sponsors must be in these domains** to ensure that only corporate employees receive the emailed link.

### **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.

A screenshot of a web-based guest registration form titled "Guest Registration" under the "ForeScout" logo. The form is set against a dark blue header with "Welcome" and a light gray background. It includes fields for "Full Name" (filled with "John Jones"), "Email Address" (filled with "John.J@ACME.com"), and "Phone" (filled with "1/22/18"). There is a "Contact Person" field (filled with "Ben Benson") and a "Contact Person Corporate Email" field with an orange annotation "Domain of this email address" pointing to it. A "Confirm Contact Person Email" field is also present. A message box states: "Ms Smith recommended that I contact you. I'll be in town until tomorrow." At the bottom, there is a "Request Access" button and a link "Already have a password? Log In".

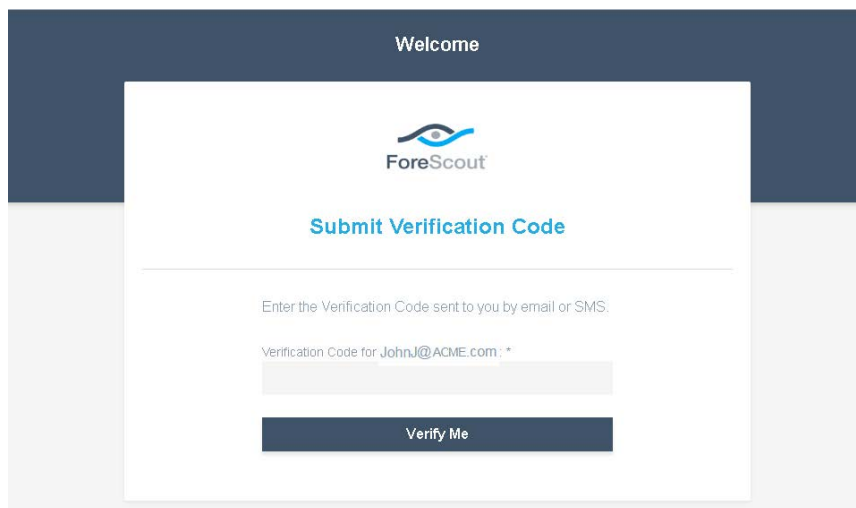
**Sample Guest Registration Form**

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***

The *HTTP Login* action requires guests to register before the Guest Registration request is processed. A customizable 8-character alphanumeric verification code validates the email address or phone number entered by the guest in the Guest Registration form is valid.

The Forescout platform sends the one-time verification code to the guest email address or mobile phone number the guest entered in the registration form. The guest must enter that code in the Guest Verification Code Form before logging in to the network. Verification codes are automatically generated and validated by the Forescout platform.

A screenshot of a web form titled "Submit Verification Code" from the ForeScout platform. The form is centered on a dark blue background with a "Welcome" header. The ForeScout logo is at the top. Below the title, there is a text input field with the placeholder "Enter the Verification Code sent to you by email or SMS." and a label "Verification Code for John.J@ACME.com; \*". A dark blue "Verify Me" button is at the bottom.

### Sample Guest Verification Code Form

Verification codes are automatically generated and validated by Forescout platform.

#### To work with verification codes:

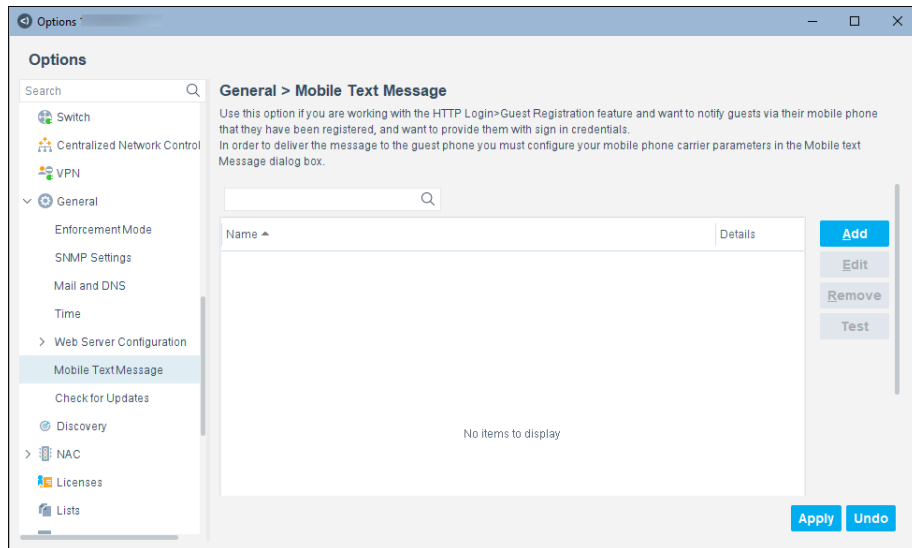
1. Select **Require Verification Code** in the *Guests* tab.
2. From the dropdown list, select whether the verification code will be sent via email only, via mobile phone only, or via both email and mobile phone. The email messages includes a customized message. The mobile text message includes only 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.



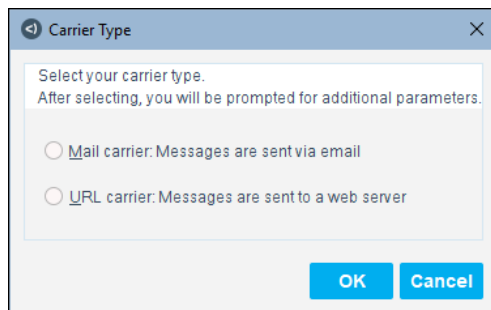
To define text messaging through a mobile carrier:

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



Mobile Text Message Pane

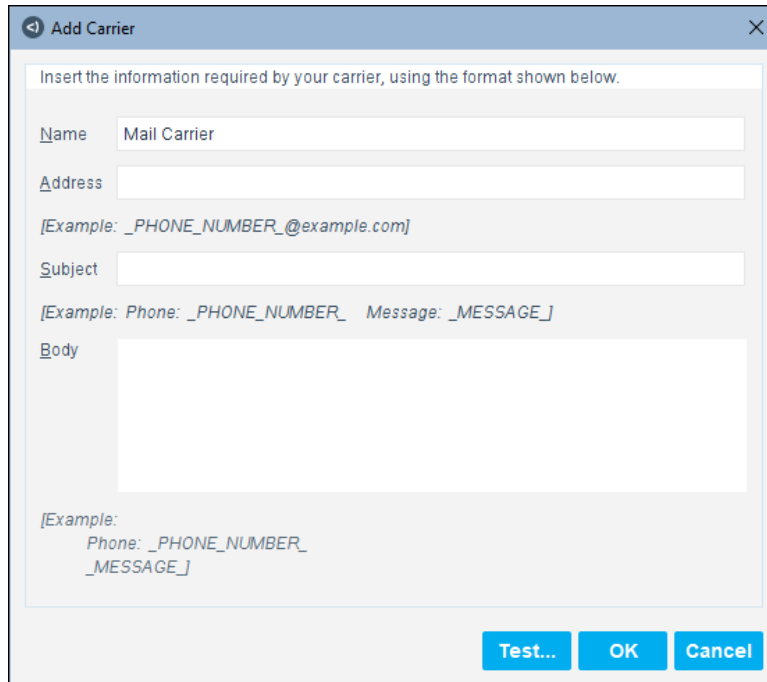
4. Select **Add**. The *Carrier Type* dialog box opens.



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.

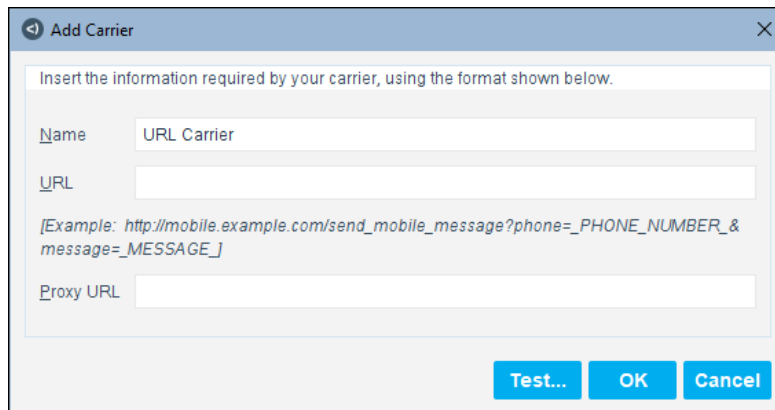
5. Select **OK**. In the Add Carrier dialog box, enter a name that identifies this carrier in the *Name* field. In the other fields of the dialog box, enter string patterns that define the format used to submit message requests.
  - For message requests in email format, the fields correspond to the Address, Subject, and Message fields of an email message.



The screenshot shows a dialog box titled "Add Carrier" with a close button (X) in the top right corner. Inside the dialog, there is a text area at the top with the instruction: "Insert the information required by your carrier, using the format shown below." Below this, there are four input fields: "Name" (containing "Mail Carrier"), "Address", "Subject", and "Body". Below the "Address" field, there is an example text: "[Example: \_PHONE\_NUMBER\_@example.com]". Below the "Subject" field, there is an example text: "[Example: Phone: \_PHONE\_NUMBER\_ Message: \_MESSAGE\_]". Below the "Body" field, there is an example text: "[Example: Phone: \_PHONE\_NUMBER\_ \_MESSAGE\_]". At the bottom right of the dialog, there are three buttons: "Test...", "OK", and "Cancel".

**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.



The screenshot shows a dialog box titled "Add Carrier" with a close button (X) in the top right corner. Inside the dialog, there is a text area at the top with the instruction: "Insert the information required by your carrier, using the format shown below." Below this, there are three input fields: "Name" (containing "URL Carrier"), "URL", and "Proxy URL". Below the "URL" field, there is an example text: "[Example: http://mobile.example.com/send\_mobile\_message?phone=\_PHONE\_NUMBER\_&message=\_MESSAGE\_]". At the bottom right of the dialog, there are three buttons: "Test...", "OK", and "Cancel".

**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.

6. 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.
7. 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.

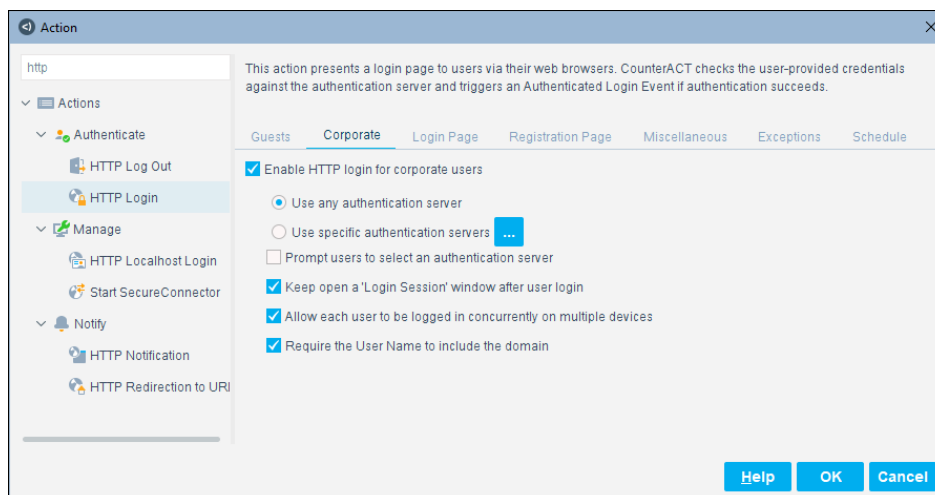
See [Managing Guest Tags](#) for detailed information about working with guest tags.

### 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 [Chapter 1: User Directory Management](#).

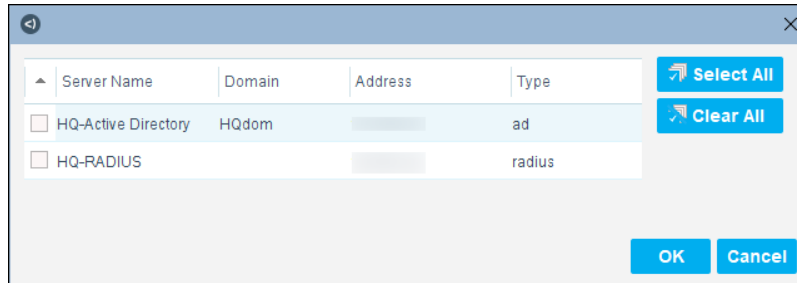


HTTP Login, Corporate Tab

To enable corporate user authentication against an authentication server, select **Enable HTTP login for corporate users**.

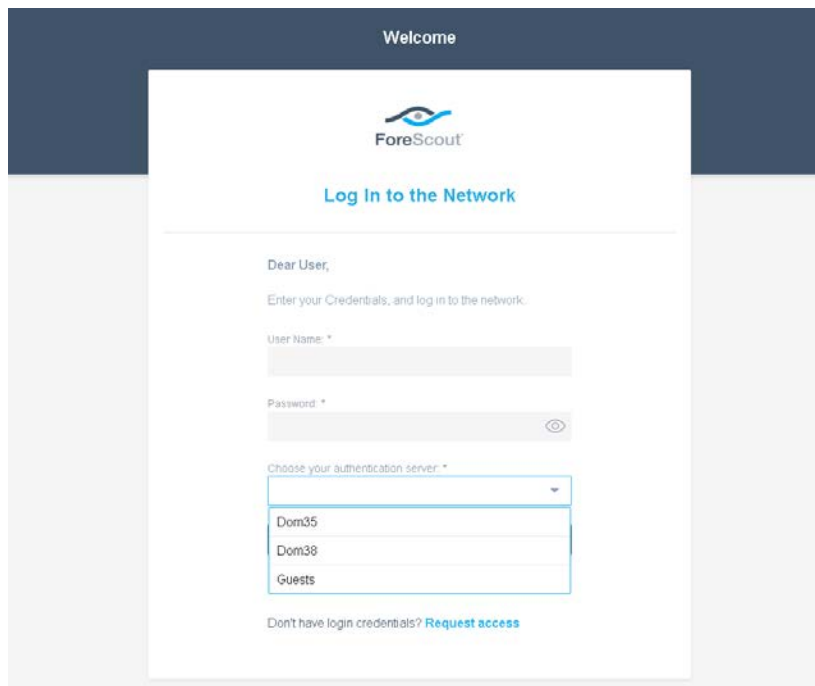
To allow authentication against any of the authentication servers that you defined in the User Directory Plugin, select **Use any authentication server**.

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**

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**

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 require corporate users to provide their domain name during authentication, select **Require the User Name to include the domain**.

### 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*.

The screenshot shows a web form titled "Guest Registration" with the ForeScout logo. The form is divided into sections by a wavy line. Above the line, the "Header" section contains the title and a "Message" to the guest. Below the line, the "Fields" section contains input fields for "Full Name", "Email Address", and "Phone". Below the fields, there is a "Contact Person" section with fields for "Contact Person", "Contact Person Corporate Email", and "Confirm Contact Person Email". A "Message for Your Contact Person" is displayed below these fields. At the bottom, there is a "Request Access" button and a link for users who already have a password.

Annotations on the form:

- Header**: Points to the "Guest Registration" title.
- Message**: Points to the text "Dear Guest, To connect to the network, complete the fields and select Request Access button."
- Fields**: Points to the input fields for "Full Name", "Email Address", and "Phone".

### 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)

This action presents a login page to users via their web browsers. CounterACT checks the user-provided credentials against the authentication server and triggers an Authenticated Login Event if authentication succeeds.

Guests Corporate Login Page **Registration Page** Miscellaneous Exceptions Schedule

Header: Guest Registration

Registration Instructions: <b>Dear Guest,</b>  
To connect to the network, complete the fields and select <b>Request Access</b> button.

☐ Require Registration Code  
☐ Enable automatic login  
☒ Allow invalid email addresses

Full Name	Mandatory
Phone	Show
Company	Show
Title	Show
Location	Show
Contact Person	Show
Contact Person Email	Show
Contact Person Email Confirmation	Mandatory
Time Frame	Show
Comment	Show
Custom1	Hide
Custom2	Hide
Custom3	Hide
Custom4	Hide
Custom5	Hide
Custom6	Hide

Tags: Add Tags

Help OK Cancel

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.

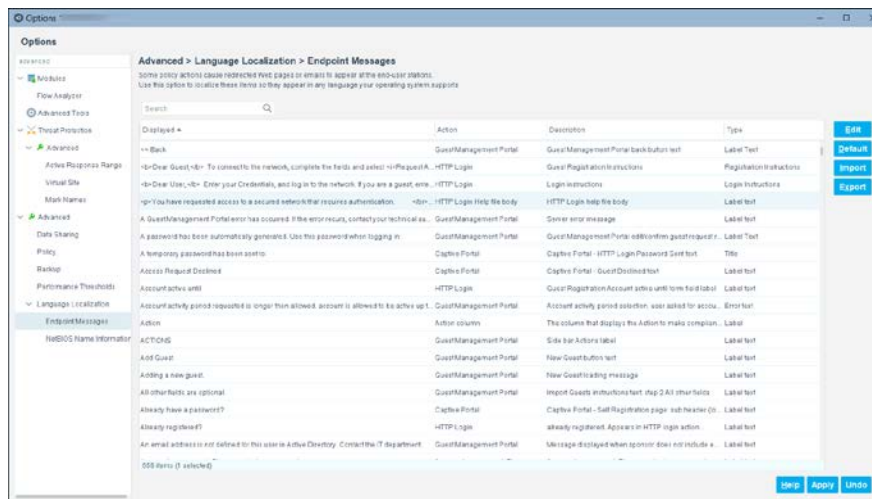
7. If tags are defined in your environment, you can select tags to be added to the Guest Registration form.

☞ *SMS must be disabled to hide the Phone field on the Guest Registration page. See [Registration Page Tab](#).*

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 will be located.

### To assign custom names:

1. Select **Options** from the Console **Tools** menu and then select **Advanced > Language Localization > Endpoint Messages**.
2. Type the word *Custom* in the search field.



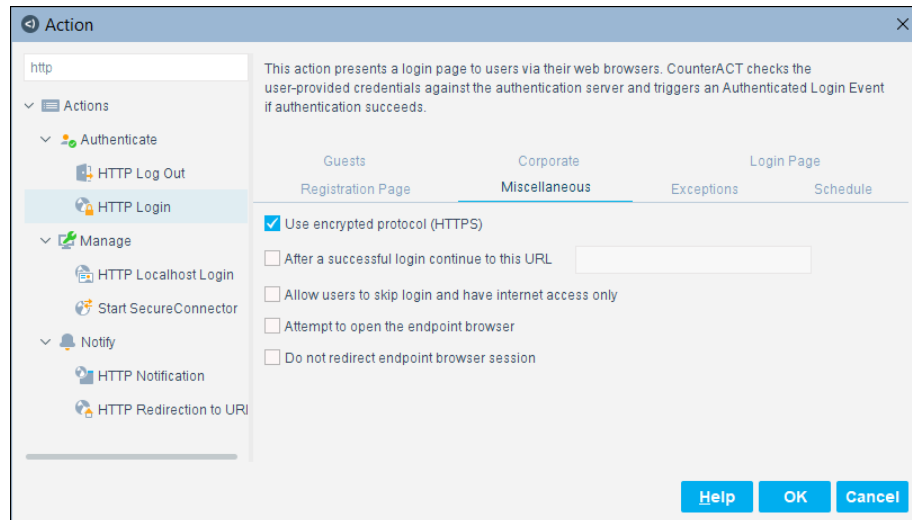
### Localization

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

### *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:

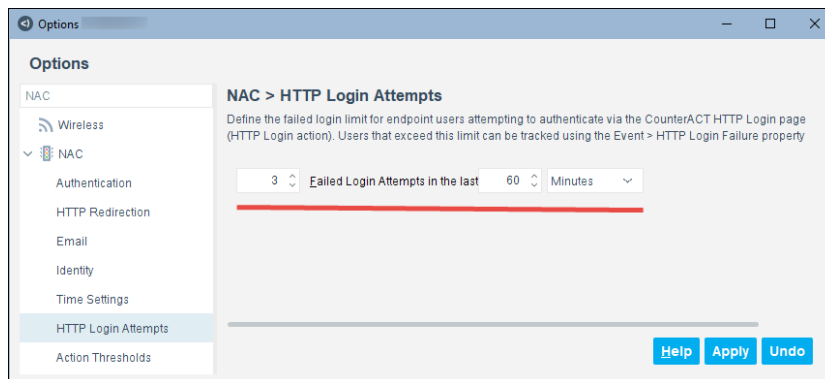
- Guest verification code
- HTTP Login (with or without other values)
- HTTP Login mobile

## **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:**

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



5. 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.
6. 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.

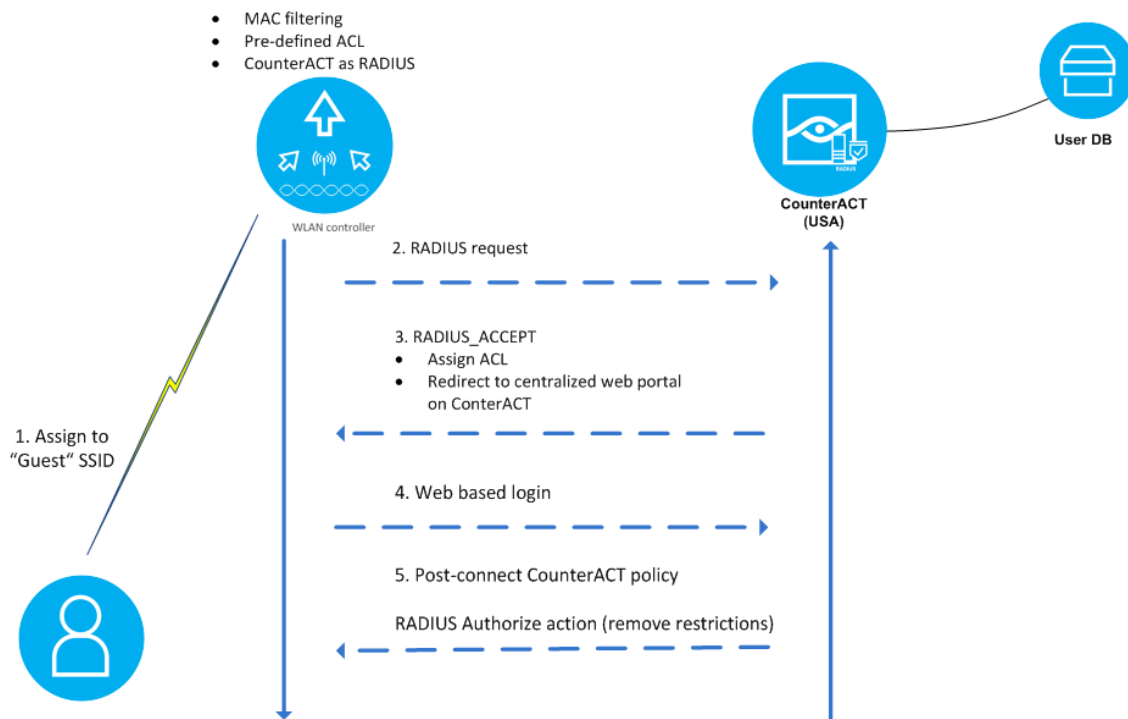
### Hijack Methods

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

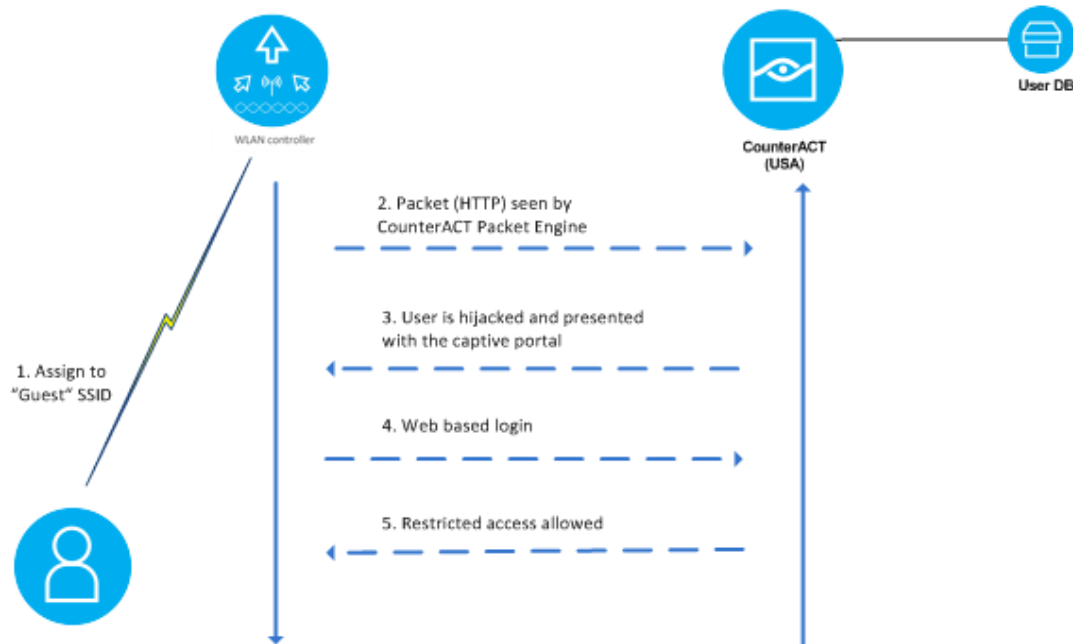
Forescout platform centralized web authentication combines the use of both MAC authentication (provided by the RADIUS Plugin) and Forescout policy actions to authenticate endpoints.



#### 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.*

## Guest Management Interface Customization

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

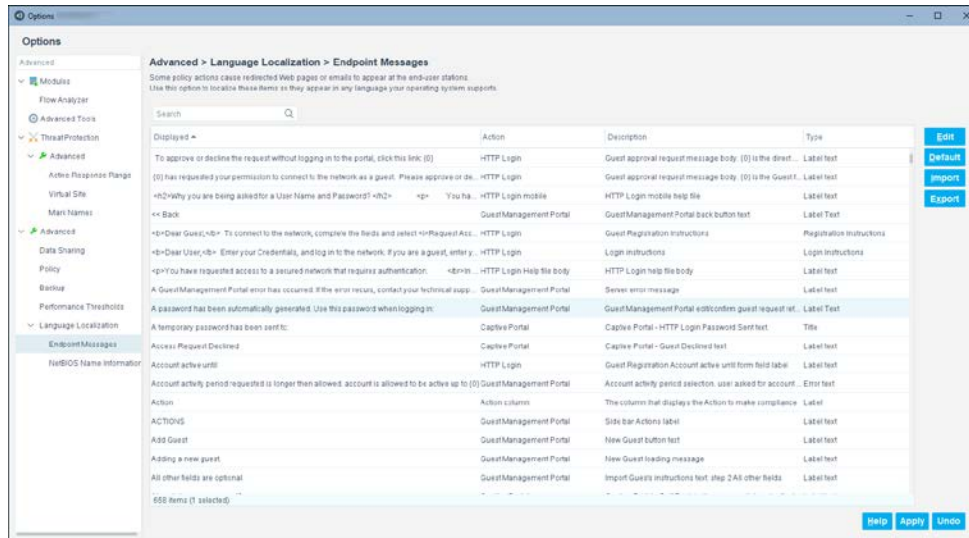
### Localize Web Pages and Messages

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:

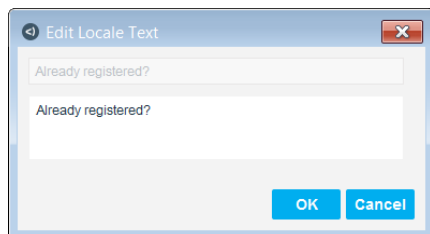
1. Select **Options** from the Console **Tools** menu and then select **Advanced > Language Localization > Endpoint Messages**.

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



### Localization > Endpoint Messages Pane

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.




### Edit Locale Text

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**.

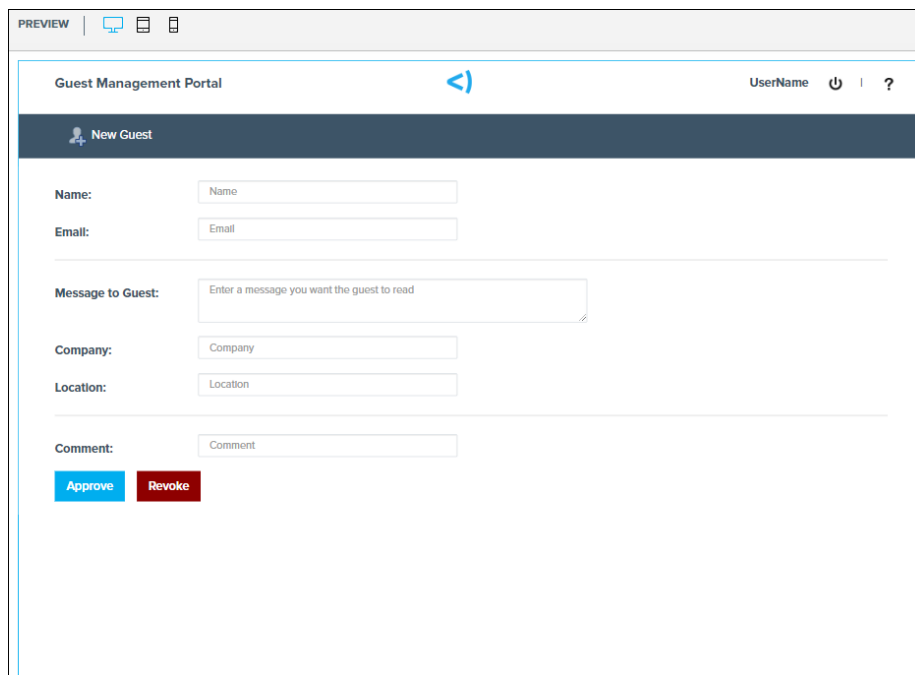
## The Forescout User Portal Builder

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

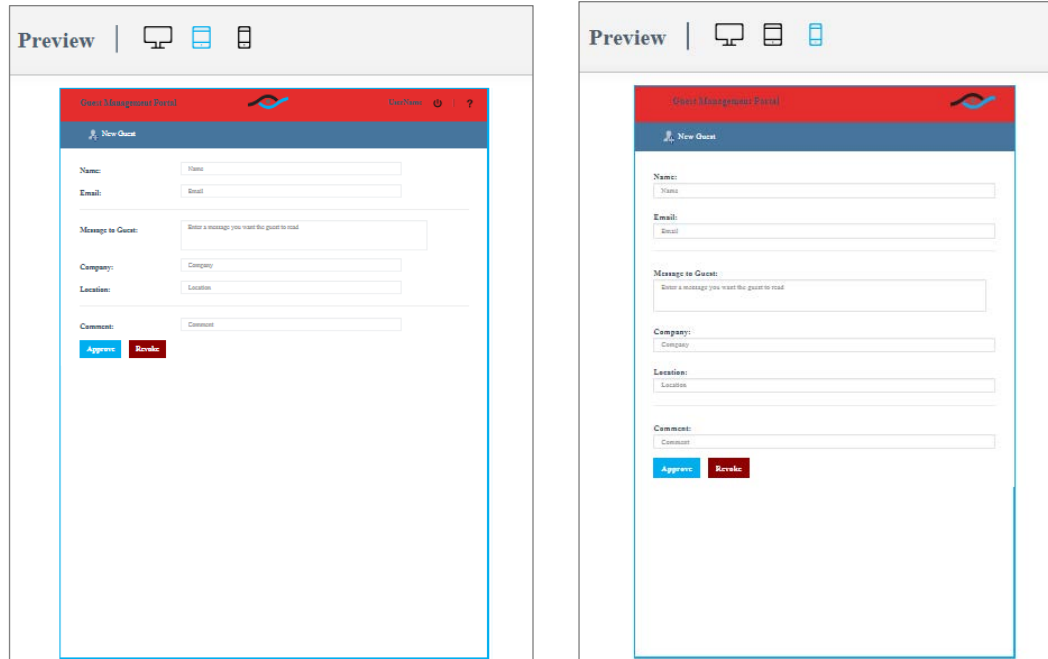
- HTTP Notification
- HTTP Login
- Guest Management Portal

 *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.



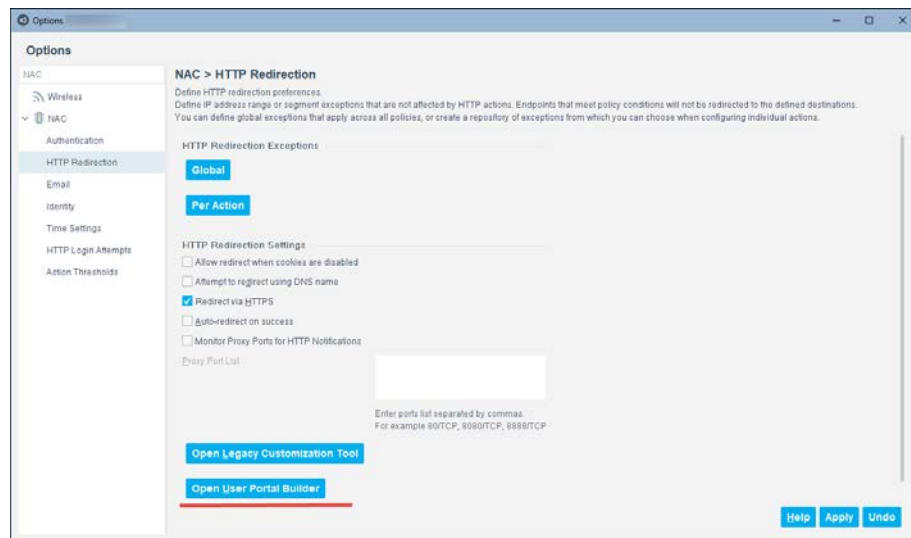
The screenshot shows a web browser window with a 'PREVIEW' tab selected. The browser address bar shows a local address. The page title is 'Guest Management Portal'. The header bar includes a back arrow icon, the text 'UserName', a power icon, and a question mark icon. Below the header is a dark blue bar with a person icon and the text 'New Guest'. The main content area contains several form fields: 'Name:' with a text input labeled 'Name'; 'Email:' with a text input labeled 'Email'; 'Message to Guest:' with a text area labeled 'Enter a message you want the guest to read'; 'Company:' with a text input labeled 'Company'; 'Location:' with a text input labeled 'Location'; and 'Comment:' with a text input labeled 'Comment'. At the bottom of the form are two buttons: 'Approve' (blue) and 'Revoke' (red).




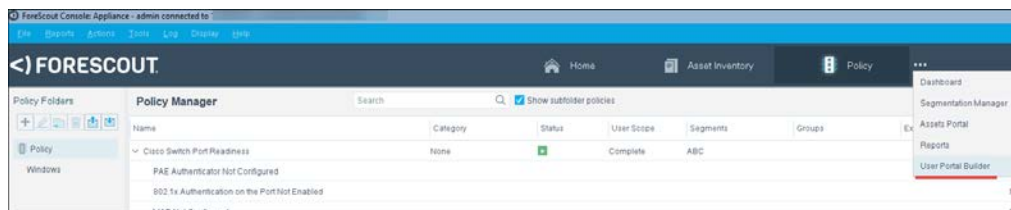
## Opening the User Portal Builder

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

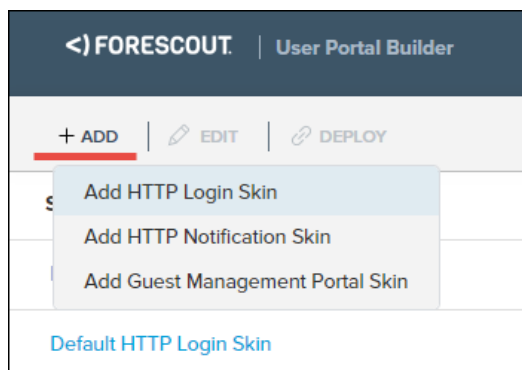
The User Portal Builder provides a simple way to edit and preview:

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

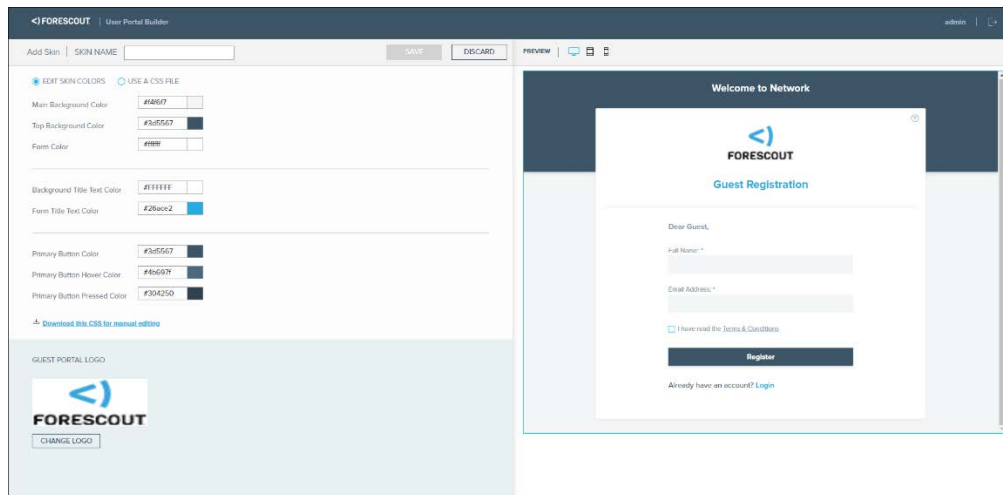
New skins can be added, and skins that were added can be edited.

### To add a new skin:


1. In the *User Portal Builder*, select **Add**.

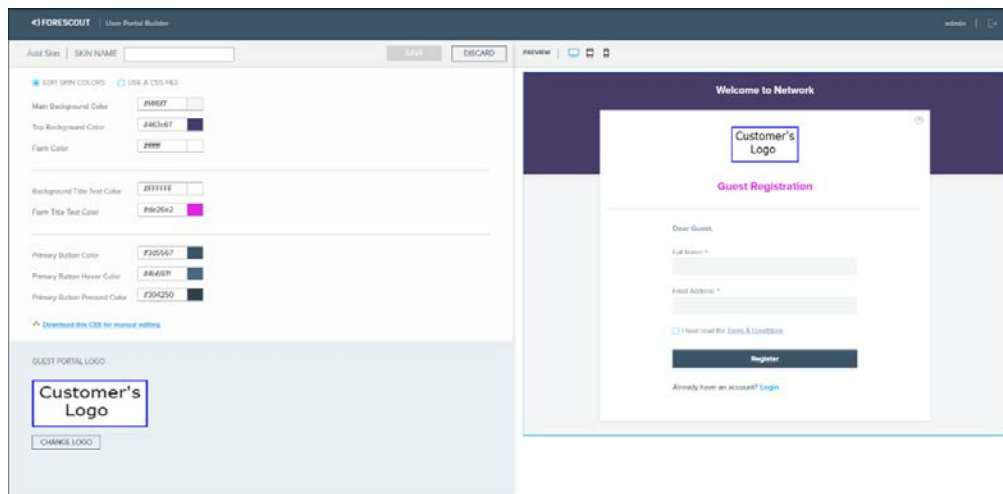


2. Select the user interface:
  - **Add HTTP Login Skin** to customize the HTTP Login window.
  - **Add HTTP Notification Skin** to customize the HTTP Notification window.
  - **Add Guest Management Skin** to customize the Guest Management Portal.
3. A copy of the default skin opens for you to edit.



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

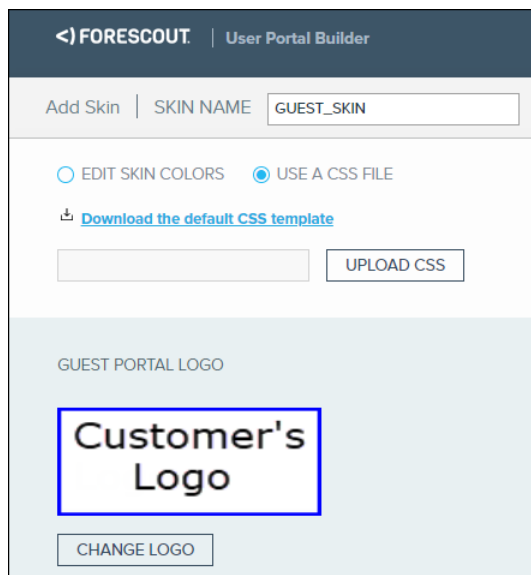
You may want to configure user interface features that are not included in the User Portal Builder basic customization. For example:

- 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**.





The screenshot shows the 'FORESCOUT | User Portal Builder' interface. At the top, there's a header with the FORESCOUT logo and the title 'User Portal Builder'. Below the header, there's a section for 'Add Skin' with a 'SKIN NAME' input field containing 'GUEST\_SKIN'. Underneath, there are two radio buttons: 'EDIT SKIN COLORS' (unselected) and 'USE A CSS FILE' (selected). Below these, there's a link 'Download the default CSS template' with a download icon. A file upload area with a text input field and an 'UPLOAD CSS' button is also present. The bottom section is titled 'GUEST PORTAL LOGO' and features a placeholder image with the text 'Customer's Logo' inside a blue border. Below the placeholder is a 'CHANGE LOGO' button.

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**.

The screenshot shows the FORESCOUT User Portal Builder interface. On the left, a table lists available skins. On the right, a preview of the 'Guest Registration' form is shown.

SKIN NAME	TYPE	STATUS	LAST MODIFIED
Default HTTP Notification Skin	HTTP Notification	✓ Deployed	
Default HTTP Login Skin	HTTP Login	✓ Deployed	
Default Guest Management Portal Skin	Guest Management Portal	✓ Deployed	
GUEST_LOGIN_COLORS	HTTP Login	Not Deployed	Nov 28, 2019 6:51:05 PM

The preview on the right shows a 'Welcome to Network' header with a 'Customer's Logo' placeholder. Below is a 'Guest Registration' form with fields for 'Full Name' and 'Email Address', a checkbox for 'I have read the Terms & Conditions', a 'Register' button, and a link for 'Already have an account? Login'.