End User Configuration

The following topics contain information on managing end user directory information:

- End User Configuration Settings, page 88-1
- Creating a Cisco Unity Connection Voice Mailbox, page 88-7
- Changing an End User Password, page 88-9
- Changing an End User PIN, page 88-9
- Managing End User Credential Information, page 88-10
- Credential Settings and Fields, page 88-10
- Configuring User-Related Information for End Users, page 88-11
- Associating Devices to an End User, page 88-12
- Associating Cisco Extension Mobility Profiles, page 88-14
- Related Topics, page 88-15

End User Configuration Settings

In Cisco Unified Communications Manager Administration, use the User Management > End User menu path to configure end users.

The End User Configuration window in Cisco Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window.

Tips About Configuring End Users

Consult the following information before you begin to configure end users:

- To verify whether the Enable Synchronizing from LDAP Server check box is checked, choose System > LDAP > LDAP System. If the check box is checked, LDAP synchronization is enabled; if not, LDAP synchronization is disabled.
- If you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you thereby configure your system to use the LDAP corporate directory as the end user directory for Cisco Unified Communications Manager. In this scenario, you cannot add or delete users in Cisco Unified Communications Manager Administration. You add and remove end users in the corporate LDAP directory.
End User Configuration Settings

- If you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you cannot change some existing user information, including user IDs, in the End User Configuration windows. Instead, you must use the corporate LDAP directory to update some user information.

- If you configure your system to authenticate users against the LDAP directory, you cannot configure or change end user passwords in Cisco Unified Communications Manager Administration. Instead, you must use the corporate LDAP directory.

- You can import Cisco Unity Connection users in Cisco Unity Connection, as described in the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Or, if you want to do so, you can configure a Cisco Unified Communications Manager Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window, as described in the “Creating a Cisco Unity Connection Voice Mailbox” section on page 88-7. You can then configure any additional settings in Cisco Unity Connection Administration.

**Note** Before you can create a Cisco Unity Connection mailbox for the end user, you must configure the end user with a phone device association and a primary extension, and the integration between Cisco Unified Communications Manager and Cisco Unity Connection must be complete. For more information, see the Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection or the Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection.

**Next Steps in Configuring an End User**

If you want to associate devices to this end user, continue with the “Associating Devices to an End User” procedure.

To manage credentials for this end user, continue with the “Managing End User Credential Information” procedure.

To create a Cisco Unity Connection Voice Mailbox for this user in Cisco Unified Communications Manager Administration, continue with the procedure in “Creating a Cisco Unity Connection Voice Mailbox” section on page 88-7.

**Tips About Deleting End Users**

Before you delete an end user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

You can view the devices and profiles that are assigned to the end user from the Device Associations, Extension Mobility, Directory Number Associations, CAPF Information, and Permissions Information areas of the End User Configuration window. You can also choose **Dependency Records** from the Related Links drop-down list box in the End User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2.

**Next Steps in Deleting an End User**

If this user is configured in Cisco Unity Connection, the user association to Cisco Unified Communications Manager gets broken when you delete the user in Cisco Unified Communications Manager Administration. You can delete the orphaned user in Cisco Unity Connection Administration. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. Deleting the user will delete all messages in the user voice mailbox.
Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section on page 1-13 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 88-1 describes the end user configuration settings. For related procedures, see the “Related Topics” section on page 88-15.

<table>
<thead>
<tr>
<th>Table 88-1 End User Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>User Information</strong></td>
</tr>
<tr>
<td>LDAP Sync Status</td>
</tr>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>Password / Edit Credential</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>PIN / Edit Credential</td>
</tr>
<tr>
<td>Confirm PIN</td>
</tr>
<tr>
<td>Last Name</td>
</tr>
<tr>
<td>Middle Name</td>
</tr>
<tr>
<td>First Name</td>
</tr>
<tr>
<td>Telephone Number</td>
</tr>
<tr>
<td>Mail ID</td>
</tr>
</tbody>
</table>
### End User Configuration Settings

**Table 88-1  End User Configuration Settings (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager User ID</td>
<td>Enter the user ID of the end user manager ID.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Cisco Unified Communications Manager does not require that you enter a user ID that already exists in the database.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the end user department information (for example, the department number or name).</td>
</tr>
<tr>
<td>User Locale</td>
<td>From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. Cisco Unified Communications Manager uses this locale for extension mobility and the Cisco Unified CM User Options. For Cisco Extension Mobility login, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Cisco Unified Communications Manager uses the end user locale that the default device profile specifies. <strong>Note</strong> If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.</td>
</tr>
<tr>
<td>Associated PC</td>
<td>This required field applies for Cisco IP Softphone users.</td>
</tr>
<tr>
<td>Digest Credentials</td>
<td>Enter a string of alphanumeric characters. Cisco Unified Communications Manager uses the digest credentials that you specify here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. <strong>Note</strong> For more information on digest authentication, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Confirm Digest Credentials</td>
<td>To confirm that you entered the digest credentials correctly, re-enter the credentials in this field.</td>
</tr>
<tr>
<td>Device Associations</td>
<td></td>
</tr>
<tr>
<td>Controlled Devices</td>
<td>After the device is associated, this field displays the description information (for example, the MAC address) that the end user controls. This field displays after you create a user in the database. To associate a device with this end user, click the Device Association button. See the “Associating Devices to an End User” section on page 88-12 for a detailed procedure.</td>
</tr>
<tr>
<td>Extension Mobility</td>
<td></td>
</tr>
<tr>
<td>Available Profiles</td>
<td>This list box displays the extension mobility profiles that are available for association with this end user. To search for an extension mobility profile, click Find. Use the Find and List Device Profiles window that displays to search for the extension mobility profile that you want. To associate an extension mobility profile with this end user, select the profile and click the Down arrow below this list box.</td>
</tr>
<tr>
<td>Controlled Profiles</td>
<td>This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.</td>
</tr>
<tr>
<td>Default Profile</td>
<td>From the drop-down list box, choose a default extension mobility profile for this end user.</td>
</tr>
</tbody>
</table>
Presence Group
Configure this field with the Presence feature.
From the drop-down list box, choose a Presence group for the end user. The selected group specifies the destinations that the end user can monitor.
The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box.
Presence authorization works with presence groups to allow or block presence requests between groups. See the “Presence” chapter in the Cisco Unified Communications Manager Features and Services Guide for information about configuring permissions between groups and how presence works with extension mobility.

SUBSCRIBE Calling Search Space
Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.
From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box.
If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.
To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. For information on how to configure a calling search space, see the “Calling Search Space Configuration” section on page 41-1

Allow Control of Device from CTI
If this check box is checked, when the user logs in to a device, the AllowCTIControlFlag device property becomes active, which allows control of the device from CTI applications. Until the user logs in to a device, this setting has no effect.

Note
The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user logs in.

Enable Extension Mobility Cross Cluster
Check this box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.
For more information about the Cisco Extension Mobility Cross Cluster feature, see the “Cisco Extension Mobility Cross Cluster” chapter of the Cisco Unified Communications Manager Features and Services Guide.

Directory Number Associations
Primary Extension
This field represents the primary directory number for the end user. End users can have multiple lines on their phones.
When you associate devices to the end user, directory numbers that are configured on the associated device become available in the drop-down list box for Primary Extension. From the drop-down list box, choose a primary extension for this end user.
If the system is integrated with Cisco Unity Connection, the Create Cisco Unity User link displays in the Related Links menu.

Table 88-1  End User Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence Group</td>
<td>Configure this field with the Presence feature. From the drop-down list box,</td>
</tr>
<tr>
<td></td>
<td>choose a Presence group for the end user. The selected group specifies the</td>
</tr>
<tr>
<td></td>
<td>destinations that the end user can monitor. The default value for Presence</td>
</tr>
<tr>
<td></td>
<td>Group specifies Standard Presence group, configured with installation. Presence</td>
</tr>
<tr>
<td></td>
<td>groups that are configured in Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>Administration also appear in the drop-down list box. Presence authorization</td>
</tr>
<tr>
<td></td>
<td>works with presence groups to allow or block presence requests between groups.</td>
</tr>
<tr>
<td></td>
<td>See the “Presence” chapter in the Cisco Unified Communications Manager Features</td>
</tr>
<tr>
<td></td>
<td>and Services Guide for information about configuring permissions between groups</td>
</tr>
<tr>
<td></td>
<td>and how presence works with extension mobility.</td>
</tr>
<tr>
<td>SUBSCRIBE Calling</td>
<td>Supported with the Presence feature, the SUBSCRIBE calling search space</td>
</tr>
<tr>
<td>Search Space</td>
<td>determines how Cisco Unified Communications Manager routes presence requests</td>
</tr>
<tr>
<td></td>
<td>that come from the end user. This setting allows you to apply a calling</td>
</tr>
<tr>
<td></td>
<td>search space separate from the call-processing search space for presence</td>
</tr>
<tr>
<td></td>
<td>(SUBSCRIBE) requests for the end user. From the drop-down list box, choose the</td>
</tr>
<tr>
<td></td>
<td>SUBSCRIBE calling search space to use for presence requests for the end user.</td>
</tr>
<tr>
<td></td>
<td>All calling search spaces that you configure in Cisco Unified Communications</td>
</tr>
<tr>
<td></td>
<td>Manager Administration display in the SUBSCRIBE Calling Search Space drop-down</td>
</tr>
<tr>
<td></td>
<td>list box. If you do not select a different calling search space for the end</td>
</tr>
<tr>
<td></td>
<td>user from the drop-down list, the SUBSCRIBE calling search space defaults to</td>
</tr>
<tr>
<td></td>
<td>None. To configure a SUBSCRIBE calling search space specifically for this</td>
</tr>
<tr>
<td></td>
<td>purpose, you configure a calling search space as you do all calling search</td>
</tr>
<tr>
<td></td>
<td>spaces. For information on how to configure a calling search space, see the</td>
</tr>
<tr>
<td></td>
<td>“Calling Search Space Configuration” section on page 41-1.</td>
</tr>
<tr>
<td>Allow Control of Device</td>
<td>If this check box is checked, when the user logs in to a device, the AllowCTI-</td>
</tr>
<tr>
<td>from CTI</td>
<td>ControlFlag device property becomes active, which allows control of the device</td>
</tr>
<tr>
<td></td>
<td>from CTI applications. Until the user logs in to a device, this setting has no</td>
</tr>
<tr>
<td></td>
<td>effect. The Allow Control of Device from CTI setting in the end user</td>
</tr>
<tr>
<td></td>
<td>configuration overrides the AllowCTIControlFlag device property of the device</td>
</tr>
<tr>
<td></td>
<td>to which the user logs in.</td>
</tr>
<tr>
<td>Enable Extension</td>
<td>Check this box to enable this end user to use the Cisco Extension Mobility</td>
</tr>
<tr>
<td>Mobility Cross Cluster</td>
<td>Cross Cluster feature. For more information about the Cisco Extension Mobility</td>
</tr>
<tr>
<td></td>
<td>Cross Cluster feature, see the “Cisco Extension Mobility Cross Cluster” chapter</td>
</tr>
<tr>
<td></td>
<td>of the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Primary Extension</td>
<td>This field represents the primary directory number for the end user. End users</td>
</tr>
<tr>
<td></td>
<td>can have multiple lines on their phones. When you associate devices to the</td>
</tr>
<tr>
<td></td>
<td>end user, directory numbers that are configured on the associated device become</td>
</tr>
<tr>
<td></td>
<td>available in the drop-down list box for Primary Extension. From the drop-down</td>
</tr>
<tr>
<td></td>
<td>list box, choose a primary extension for this end user. If the system is</td>
</tr>
<tr>
<td></td>
<td>integrated with Cisco Unity Connection, the Create Cisco Unity User link</td>
</tr>
<tr>
<td></td>
<td>displays in the Related Links menu.</td>
</tr>
</tbody>
</table>
Chapter 88  End User Configuration

End User Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCC Extension</td>
<td>From the drop-down list box, choose an IPCC extension for this end user. Note: This field displays only if the IPCC Express Installed enterprise parameter is set to True.</td>
</tr>
</tbody>
</table>

**Mobility Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mobility</td>
<td>Check this check box to activate Mobile Connect, which allows the user to manage calls by using a single phone number and to pick up in-progress calls on the desktop phone and cellular phone. Checking this check box, which triggers licensing to consume device license units for Mobile Connect, works in conjunction with the Primary User Device drop-down list box. If you check the Enable Mobility check box and fail to choose an adjunct device from the Primary User Device drop-down list box, four device license units (DLUs) get consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window. If you enable Cisco Unified Mobility and later choose an adjunct device from the Primary User Device drop-down list box, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.</td>
</tr>
</tbody>
</table>
| Primary User Device    | The Primary User Device drop-down list box, which works in conjunction with the Enable Mobility check box, controls the number of device license units that are consumed for adjunct devices for Mobile Connect. After you check the Enable Mobility check box, choose an adjunct device that you want to assign to the user specifically for Cisco Unified Mobility. For example, choose a device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility. Before you choose an adjunct device, consider the following information:  
  - Only devices that consume two or more device license units (DLUs) display in the drop-down list box.  
  - For Cisco Unified Mobility, you cannot assign the same device to multiple users, so only the devices that you can assign display in the drop-down list box.  
  - If you check the Enable Mobility check box and choose a device from the drop-down list box, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the Licensing Unit Calculator window.  
  - If you delete the device from Cisco Unified Communications Manager Administration or remove the assignment after you enable Mobile Connect, two DLUs get consumed after you delete the device or remove the assignment, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window. |
| Enable Mobile Voice Access | Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities. |
| Maximum Wait Time for Desk Pickup | Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone. |
| Remote Destination Limit | Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone. |
| Remote Destination Profiles | This field lists the remote destination profiles that have been created for this user. To view the details of a particular remote destination profile, choose a remote destination profile in the list and click the View Details link. |
Creating a Cisco Unity Connection Voice Mailbox

The “Create Cisco Unity User” link on the End User Configuration window allows you to create individual Cisco Unity Connection voice mailboxes in Cisco Unified Communications Manager Administration.
Before You Begin

- You must configure Cisco Unified Communications Manager for voice messaging.
- You must configure the Cisco Unity Connection server to use the integrated mailbox feature. See the “Creating Multiple User Accounts from Cisco Unified Communications Manager Users” chapter of the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.
- For Cisco Unity Connection integration, create an AXL connection via Cisco Unity Connection, as described in the “Managing the Phone System Integrations” chapter in the System Administration Guide for Cisco Unity Connection.
- Ensure that you have defined an appropriate template and class of service (COS) for any voice-messaging users that you plan to add in Cisco Unified Communications Manager Administration. For Cisco Unity Connection users, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.
- You must associate a device and a Primary Extension Number to the end user before the Create Cisco Unity User link displays. The link displays in the Related Links menu.
- If you want to do so, you can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in this section. For information on how to use the import feature, see the “Creating Multiple User Accounts from Cisco Unified Communications Manager Users” chapter of the User Moves, Adds, and Changes Guide for Cisco Unity Connection.

Note
The Directory Number Configuration window also displays the “Create Cisco Unity User” link in the Related Links drop-down list box.

Procedure

Step 1
Use the User Management > End User menu option to find the end user.

Step 2
Verify that a primary extension number is associated with this user.

Note
You must ensure that you have defined a primary extension; otherwise, the “Create Cisco Unity User” link will not display in the Related Links drop-down list box.

Step 3
From the Related Links drop-down list box, in the upper, right corner of the window, choose the “Create Cisco Unity User” link and click Go.

The Add Cisco Unity User dialog box displays.

Step 4
From the Application Server drop-down list box, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user and click Next.

Step 5
From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

Step 6
Click Save.

The mailbox gets created. The link in the Related Links drop-down list box changes to “Edit Cisco Unity User” in the End User Configuration window. In Cisco Unity Connection Administration, you can now view the user that you created.
Note
When the Cisco Unity Connection user is integrated with the Cisco Unified Communications Manager end user, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration); First Name; Last Name; Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Additional Information
See the “Related Topics” section on page 88-15.

Changing an End User Password

Use the following procedure to change the password for an end user in Cisco Unified Communications Manager Administration.

Note
You cannot change an end user password when LDAP authentication is enabled.

Procedure

Step 1
Use the User Management > End User menu option to find the end user.
The End User Configuration window displays the configuration information.

Step 2
In the Password field, double-click the existing password, which is encrypted, and enter the new password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 3
In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.

Step 4
Click Save.

Additional Information
See the “Related Topics” section on page 88-15.

Changing an End User PIN

Use the following procedure to change the personal identification number (PIN) for an end user.

Procedure

Step 1
Use the User Management > End User menu option to find the end user.
The End User Configuration window displays the configuration information.

Step 2
In the PIN field, double-click the existing PIN, which is encrypted, and enter the new PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).
Managing End User Credential Information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an end user. You can edit user credentials only after the user exists in the database.

In the user Credential Configuration window, you cannot save settings that conflict with the assigned credential policy.

In the user Credential Configuration window, you cannot change settings that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change check box is checked, you cannot check the User Must Change at Next Login check box.

The credential configuration window reports approximate event times; the system updates the form at the next authentication query or event.

Before You Begin
Create the end user in the database. See “End User Configuration Settings” section on page 88-1.

Procedure

Step 1 Use the User Management > End User menu option to find the end user.
The End User Configuration window displays the configuration information.

Step 2 To change or view password information, click the Edit Credential button next to the Password field.
To change or view PIN information, click the Edit Credential button next to the PIN field.

Step 3 Enter the appropriate settings as described in Table 88-2.

Step 4 If you have changed any settings, click Save.

Additional Information
See the “Related Topics” section on page 88-15.

Credential Settings and Fields

Table 88-2 describes the credential settings for end users and application users. These settings do not apply to application user or end user digest credentials. For related procedures, see the “Related Topics” section on page 88-15.
After you add a new end user, you can configure additional information that is related to the end user. This information allows each end user to personalize phone features, Manager Configuration, Assistant Configuration, Cisco Extension Mobility, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Softphone capability.
Before You Begin
Make sure that the end user is in the database.

Procedure

**Step 1** Use the User Management > End User menu option to find the end user whose application profile(s) you want to configure.

The End User Configuration window displays with information about the chosen end user.

**Step 2** Click the userid.

**Step 3** To configure a manager for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Manager Configuration and click Go.

The Manager Configuration window displays for this end user. See the “Cisco Unified Communications Manager Assistant With Proxy Line Support” and “Cisco Unified Communications Manager Assistant With Shared Line Support” chapters in the Cisco Unified Communications Manager Features and Services Guide for details of configuring Cisco Unified Communications Manager Assistant.

After you configure the Manager information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Manager Configuration window, choose Back to User Configuration and click Go.

**Step 4** To configure an assistant for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Assistant Configuration and click Go.

The Assistant Configuration window displays for this end user. See the “Cisco Unified Communications Manager Assistant With Proxy Line Support” and “Cisco Unified Communications Manager Assistant With Shared Line Support” chapters in the Cisco Unified Communications Manager Features and Services Guide for details of configuring Cisco Unified Communications Manager Assistant.

After you configure the Assistant information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Assistant Configuration window, choose Back to User Configuration and click Go.

**Step 5** To show the user privilege report for this end user, from the Related Links drop-down list box, choose User Privilege Report and click Go.

The User Privilege window displays for this end user. See the “Viewing User Roles, User Groups, and Permissions” section on page 90-7 for details of the user privilege report.

After you display the user privilege report for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the User Privilege window, choose Back to User and click Go.

Additional Information
See the “Related Topics” section on page 88-15.

**Associating Devices to an End User**

You can associate devices over which end users will have control. End users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When end users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.
Chapter 88      End User Configuration

Associating Devices to an End User

Note
For devices that are not CTI-controllable, such as H.323 devices, an asterisk (*) displays next to the device icon in the list of available devices. All device association behavior remains identical regardless of the type of device for which the feature is configured.

Before You Begin
To associate devices with an end user, you must access the End User Configuration window for that user. Use the User Management > End User menu option to find the end user. When the End User Configuration window displays, perform the following procedure to assign devices.

Do not attempt to associate devices to a new end user before you finish adding the new end user. Be sure to click Save on the End User Configuration window before you add device associations for a new end user.

Procedure

Step 1
In the Device Associations pane, click Device Association.
The User Device Association window displays.

Finding a Device
Because you may have several devices in your network, Cisco Unified Communications Manager lets you locate specific devices on the basis of specific criteria. Use the following steps to locate devices.

Note
During your work in a browser session, Cisco Unified Communications Manager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your search preferences until you modify your search or close the browser.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3
Click Find.
All or matching records display. You can change the number of items that display in each window by choosing a different value from the Rows per Page drop-down list box.

Associating a Device

Step 4
From the Device association for (this particular user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device name(s).

Use the buttons at the bottom of the window to select and deselect devices to associate with the end user.
The buttons function to select and deselect only the devices that were found as a result of any search for devices that you performed in the preceding steps.

Tip
Check the Show the devices already associated with user check box to display the devices that are already associated with this end user.

Use the buttons to perform the following functions:

- **Select All**—Click this button to select all devices that display in this window.
- **Clear All**—Click this button to uncheck the check boxes next to all devices that display in this window.
- **Select All in Search**—Click this button to select all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and selects all the matching devices.
- **Clear All in Search**—Click this button to deselect all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and deselects all the matching devices.
- **Save Selected/Changes**—Click this button to associate the devices that you have selected with this end user.
- **Remove All Associated Devices**—Click this button to disassociate all devices that are already associated with this end user. After you click this button, a popup window asks you to confirm that you want to remove all device associations from this end user. To confirm, click OK.

**Step 5**
Repeat the preceding steps for each device that you want to assign to the end user.

**Step 6**
To complete the association, click **Save Selected/Changes**.

**Step 7**
From Related Links drop-down list box in the upper, right corner of the window, choose **Back to User**, and click **Go**.

The End User Configuration window displays, and the associated devices that you chose display in the Controlled Devices pane.

---

**Additional Information**
See the “Related Topics” section on page 88-15.

---

**Associating Cisco Extension Mobility Profiles**

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone to temporarily display as the phone of an end user. The end user can log in to a phone, and the extension mobility profile (including line and speed-dial numbers) for the end user resides on the phone. This feature applies primarily in environments where end users are not permanently assigned to physical phones.

To associate an extension mobility profile to an end user, you must access the End User Configuration window for that end user. Use the **User Management > End User** menu option to find the end user. To configure and associate Cisco Extension Mobility for end users, see the “Cisco Extension Mobility” chapter in the *Cisco Unified Communications Manager Features and Services Guide*. 
Additional Information
See the “Related Topics” section on page 88-15.

Related Topics

- End User Configuration Settings, page 88-1
- Creating a Cisco Unity Connection Voice Mailbox, page 88-7
- Changing an End User Password, page 88-9
- Changing an End User PIN, page 88-9
- Managing End User Credential Information, page 88-10
- Credential Settings and Fields, page 88-10
- Configuring User-Related Information for End Users, page 88-11
- Associating Devices to an End User, page 88-12
- Associating Cisco Extension Mobility Profiles, page 88-14
- Application User Configuration Settings, page 87-1
- Adding an Administrator User to Cisco Unity or Cisco Unity Connection, page 87-6
- Changing an Application User Password, page 87-8
- Managing Application User Credential Information, page 87-8
- Credential Settings and Fields, page 87-9
- Associating Devices to an Application User, page 87-10
- LDAP System Configuration, page 11-1
- Role Configuration, page 89-1
- User Group Configuration, page 90-1
- Viewing User Roles, User Groups, and Permissions, page 90-7
- Directory Number Configuration, page 43-1
- CTI Route Point Configuration, page 64-1
- Cisco Unified IP Phone Configuration, page 67-1
- Credential Policy Configuration, page 86-1
- Credential Policy Default Configuration, page 85-1
- Credential Policy, Cisco Unified Communications Manager System Guide
- Application Users and End Users, Cisco Unified Communications Manager System Guide
- Cisco Extension Mobility, Cisco Unified Communications Manager Features and Services Guide
- Cisco Extension Mobility Cross Cluster, Cisco Unified Communications Manager Features and Services Guide
- Device Association, Cisco Unified Communications Manager System Guide
- Associating a User Device Profile to a User, Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified Communications Manager Assistant With Proxy Line Support, Cisco Unified Communications Manager Features and Services Guide
• Cisco Unified Communications Manager Assistant With Shared Line Support, *Cisco Unified Communications Manager Features and Services Guide*

• Cisco Unity Messaging Integration, *Cisco Unified Communications Manager System Guide*

• Presence, *Cisco Unified Communications Manager Features and Services Guide*

**Related Documentation**

• *Cisco Unified Communications Manager Security Guide*

• *User Moves, Adds, and Changes Guide for Cisco Unity Connection*