CHAPTER 114

End User Configuration

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.

- If you configure your system to use the LDAP corporate directory as the end user directory for Cisco Unified Communications Manager, you cannot add or delete users in Cisco Unified Communications Manager Administration.You add and remove end users in the corporate LDAP directory.
- 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. You configure and change end user passwords in the corporate LDAP directory.

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

- End User Configuration Settings, page 114-1
- Finding an End User, page 114-8
- Configuring an End User, page 114-9
- Creating a Cisco Unity Connection Voice Mailbox, page 114-10
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Credential Settings and Fields, page 114-13
- Configuring User-Related Information for End Users, page 114-14
- Associating Devices to an End User, page 114-15
- Associating Cisco Extension Mobility Profiles, page 114-17
- Deleting an End User, page 114-17
- Related Topics, page 114-18

End User Configuration Settings

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.

Table 114-1 describes the end user configuration settings. For related procedures, see the "Related Topics" section on page 114-18.

Before You Begin

- If you enable LDAP synchronization in Cisco Unified Communications Manager Administration, you cannot add an end user, delete an end user, or change some existing user information, including user IDs, in the End User Configuration windows. Instead, you must add, update some user information, and delete end users in the corporate LDAP directory. To verify that the Enable Synchronizing from LDAP Server check box is not checked, choose **System > LDAP > LDAP System**.
- 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. You configure and change end user passwords in 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 114-10.

Table 114-1 End User Configuration Settings

Field	Description
User Information	
LDAP Sync Status	This field displays the LDAP synchronization status, which you set with the **System > LDAP > LDAP System** menu option.
User ID	Enter the unique end user identification name. You can enter any character, including alphanumeric and special characters. No character restrictions exist for this field. You can modify User ID only if synchronization with an LDAP server is not enabled. If synchronization is enabled, you can view the user ID, but you cannot modify it. If synchronization is disabled, Cisco Unified Communications Manager permits you to modify the user ID after it is created.
Password / Edit Credential	This field does not display if LDAP Authentication is enabled. Enter alphanumeric or special characters for the end user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The **Edit Credential** button displays after this user is added to the database. Click the **Edit Credential** button to manage credential information for this user. See the "Managing End User Credential Information" section on page 114-12.
Confirm Password	This field does not display if LDAP Authentication is enabled. Enter the end user password again.

Table 114-1 End User Configuration Settings (continued)

Field	Description
PIN / Edit Credential	Enter numeric characters for the end user PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The **Edit Credential** button displays after you add this user to the database. Click the **Edit Credential** button to manage credential information for this user. See the "Managing End User Credential Information" section on page 114-12.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name.
Middle Name	Enter the end user middle name.
First Name	Enter the end user first name.
Telephone Number	Enter the end user telephone number. You may use the following special characters: (,), and -.
Mail ID	Enter the end user e-mail address.
Manager User ID	Enter the user ID of the end user manager ID. The manager user ID that you enter must already exist in the directory as an end user.
Department	Enter the end user department information (for example, the department number or name).
User Locale	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 log on, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility log off, Cisco Unified Communications Manager uses the end user locale that the default device profile specifies. **Note** 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.
Associated PC	This required field applies for Cisco IP Softphone and Cisco Unified Communications Manager Attendant Console users.
Digest Credentials	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. **Note** For more information on digest authentication, refer to the *Cisco Unified Communications Manager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, re-enter the credentials in this field.

Table 114-1 End User Configuration Settings (continued)

Field	Description
Device Associations	
Controlled Devices	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 114-15 for a detailed procedure.
Extension Mobility	
Available Profiles	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.
Controlled Profiles	This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.
Default Profile	From the drop-down list box, choose a default extension mobility profile for this end user.
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. Refer to 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.

Table 114-1 End User Configuration Settings (continued)

Field	Description
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 53-1
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.
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.
IPCC Extension	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*.

Table 114-1 End User Configuration Settings (continued)

Field	Description
Mobility Information	
Enable Mobility	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 Calculation 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 Calculation window.
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 Calculation 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 Calculation 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.

Table 114-1 End User Configuration Settings (continued)

Field	Description
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.
CAPF Information	
Associated CAPF Profiles	This pane displays the Instance ID from the CAPF Profile that you configured for this user. To view or update the profile, double-click the Instance ID or click the Instance ID to highlight it; then, click **View Details**. The End User CAPF Profile Configuration window displays with the current settings. For information on how to configure the End User CAPF Profile, refer to the *Cisco Unified Communications Manager Security Guide*.
Permissions Information	
Groups	This list box displays after an end user record has been saved. The list box displays the groups to which the end user belongs. To add the user to one or more user groups, click the **Add to User Group** button. The Find and List User Groups window opens as a separate window. Locate the groups to which you want to add the user, check the check boxes beside those groups, and click **Add Selected** at the bottom of the window. The Find and List User Groups window closes, and the End User Configuration window displays and now shows the selected groups in the Groups list box. To remove the user from a group, highlight the group in the Groups list box and click the **Remove from User Group** button. To view or update a group, double-click the group name or click the group name to highlight it; then, click **View Details**. The User Group Configuration window displays with the current settings. For more information on finding and configuring user groups, see the "User Group Configuration" section on page 116-1.
Roles	This list box displays after an end user has been added, the Groups list box has been populated, and the user record has been saved. The list box displays the roles that are assigned to the end user. To view or update a role, double-click the role name or click the role name to highlight it; then, click **View Details**. The Role Configuration window displays with the current settings. For more information on configuring roles, see the "Role Configuration" section on page 115-1.

Finding an End User

Cisco Unified Communications Manager lets you find end user information on the basis of specific criteria. Use the following procedure to find end user information.

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.

Procedure

Step 1 Choose **User Management** > **End User**.

The Find and List Users window displays. Records from an active (prior) query may also display in the window.

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, choose a search parameter.
- From the second drop-down list box, choose 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 on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 114-18.

Configuring an End User

The following procedure provides instructions on adding and configuring an end user.

Note You can add end users through Cisco Unified Communications Manager Administration only when synchronization with an LDAP server is not enabled. When synchronization is disabled, you can add new users to the Cisco Unified Communications Manager database, and you can change the settings for existing users, including the user ID. Use the **System** > **LDAP** > **LDAP System** menu option to verify that LDAP synchronization is not enabled. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked.

If you enable LDAP synchronization, you cannot add an end user, delete an end user, or change some existing user information, including user IDs, in the End User Configuration windows.

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 114-10. You can then configure any additional settings in Cisco Unity Connection Administration.

Procedure

Step 1 Choose **User Management** > **End User**.

The Find and List End Users window displays. Use the two drop-down list boxes to search for an end user.

Step 2 Click **Add New**.

The End User Configuration window displays.

Step 3 Enter the appropriate settings as described in Table 114-1.

Step 4 When you have completed the end user information, save your changes and add the end user by clicking **Save**.

Next Steps

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 114-10.

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, refer to 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*.

Additional Information

See the "Related Topics" section on page 114-18.

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. Refer to 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, refer to 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 the "Creating a Cisco Unity Connection Voice Mailbox" section on page 114-10. For information on how to use the import feature, refer to 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 Find the end user, as described in "Finding an End User" section on page 114-8.

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 114-18.

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 procedure in the “Finding an End User” section on page 114-8 to find the end user configuration.

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 114-18.

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 procedure in the "Finding an End User" section on page 114-8 to find the end user configuration.

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).

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

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 114-18.

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. For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

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 "Configuring an End User" section on page 114-9.

Procedure

Step 1 To find the end user configuration, use the procedure in the "Finding an End User" section on page 114-8.

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 114-2.

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

Additional Information

See the "Related Topics" section on page 114-18.

Credential Settings and Fields

Table 114-2 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 114-18.

Table 114-2 Application User and End User Credential Settings and Fields

Field	Description
Locked By Administrator	Check this check box to lock this account and block access for this user. Uncheck this check box to unlock the account and allow access for this user.
User Cannot Change	Check this check box to block this user from changing this credential. Use this option for group accounts. You cannot check this check box when User Must Change at Next Login check box is checked.
User Must Change at Next Login	Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when User Cannot Change check box is checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies. You cannot uncheck this check box if the policy setting specifies Never Expires.
Reset Hack Count	Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. After the counter resets, the user can try logging in again The hack count increments whenever an authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always equals 0.
Authentication Rule	Select the credential policy to apply to this user credential.
Time Last Changed	This field displays the date and time of the most recent change for this user credential.

Table 114-2 Application User and End User Credential Settings and Fields (continued)

Field	Description
Failed Logon Attempts	This field displays the number of failed logon attempts since the last successful logon, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time has expired.
Time of Last Field Logon Attempt	This field displays the date and time for the most recent failed logon attempt for this user credential.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account.
Time Locked Due to Failed Logon Attempts	This field displays the date and time that the system last locked this user account due to failed logon attempts. The associated credential policy defines lockouts due to failed logon attempts.

Configuring User-Related Information for End Users

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. See the "Finding an End User" section on page 114-8 for more information.

Procedure

Step 1 Use the procedure in the "Finding an End User" section on page 114-8 to find the end user whose application profile(s) you want to configure. Click the userid.

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

Step 2 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. Refer to 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 3 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. Refer to 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 4 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. Refer to the "Viewing User Roles, User Groups, and Permissions" section on page 116-7 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 114-18.

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.

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. See the "Finding an End User" section on page 114-8 for information on finding existing end users. 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.

Note 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 114-18.

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. See the “Finding an End User” section on page 114-8 for information on accessing information on existing end users. To configure and associate Cisco Extension Mobility for end users, refer to the “Cisco Extension Mobility” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Deleting an End User

To delete an end user in Cisco Unified Communications Manager Administration, perform the following procedure.

Before You Begin

Before you delete the 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.

Procedure

Step 1 Choose **User Management** > **End User**.

The Find and List Users window displays.

Step 2 To locate a specific end user, enter search criteria and click **Find**.

A list of end users that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the users that you want to delete and click **Delete Selected**.
- Delete all the users in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the user ID of the user that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Next Steps

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.

Additional Information

See the "Related Topics" section on page 114-18.

Related Topics

- End User Configuration Settings, page 114-1
- Finding an End User, page 114-8
- Configuring an End User, page 114-9
- Creating a Cisco Unity Connection Voice Mailbox, page 114-10
- Changing an End User Password, page 114-11
- Changing an End User PIN, page 114-11
- Managing End User Credential Information, page 114-12
- Credential Settings and Fields, page 114-13
- Configuring User-Related Information for End Users, page 114-14
- Associating Devices to an End User, page 114-15
- Associating Cisco Extension Mobility Profiles, page 114-17
- Deleting an End User, page 114-17
- Finding an Application User, page 113-5

- Configuring an Application User, page 113-6
- Adding an Administrator User to Cisco Unity or Cisco Unity Connection, page 113-7
- Changing an Application User Password, page 113-9
- Changing an Application User Password, page 113-9
- Managing Application User Credential Information, page 113-9
- Credential Settings and Fields, page 113-10
- Associating Devices to an Application User, page 113-11
- Deleting an Application User, page 113-12
- LDAP System Configuration, page 14-1
- Role Configuration, page 115-1
- User Group Configuration, page 116-1
- Viewing User Roles, User Groups, and Permissions, page 116-7
- Directory Number Configuration, page 64-1
- CTI Route Point Configuration, page 88-1
- Cisco Unified IP Phone Configuration, page 91-1
- Credential Policy Configuration, page 112-1
- Credential Policy Default Configuration, page 111-1
- Credential Policy, *Cisco Unified Communications Manager System Guide*
- Where to Find More Information, *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*
- 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*