End user setup

This chapter provides information about managing end user directory information.

About end user setup

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

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified CM end users. End users can control phones after you associate a phone in the **End User Configuration** window. You can also enable end users for IM and Presence.

End user setup tips

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 Unified CM Administration, you thereby configure your system to use the LDAP corporate directory as the end user directory for Unified CM. In this scenario, you cannot add or delete users in Unified CM Administration. You add and remove end users in the corporate LDAP directory.
- If you enable LDAP synchronization in Unified CM 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 Unified CM 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 Unified CM Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window. 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 Unified CM 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 to configure an end user

You can associate devices to this end user and manage the end user credentials.

You can create a Cisco Unity Connection Voice Mailbox for this user in Unified CM Administration.

You can specify this cluster as the home cluster for the end user.

You can configure this end user for IM and Presence service.

You can associate a service profile to this end user.

You can associate users to their line appearances for presence.

Related Topics

Manage application user credential information
Create Cisco Unity Connection voice mailbox, on page 9
Associate devices to end user, on page 14

End user deletion

Before you delete an end user, determine whether you must remove the devices or profiles that are associated with the end user.

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.

Next steps

If this user is configured in Cisco Unity Connection, the user association to Cisco Unified Communications Manager (Unified CM) is broken when you delete the user in Unified CM 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*. Deleting the user deletes all messages in the user voice mailbox.

Related Topics

Access dependency records

End user settings

The following table describes the end user settings.

Table 1: End user 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 the 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 (Unified CM) permits you to modify the user ID after you create it.
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.
Confirm Password	This field does not display if LDAP Authentication is enabled. Enter the end user password again.

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 appears after you add this user to the database. Click the Edit Credential button to manage credential information for this user.
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.
Directory URI	Enter the directory URI that you want to associate to this end user. A directory URI looks like an email address and follows the user@host format. For information about valid formats for directory URIs, see Directory URI formats in the "Intercluster Directory URI" chapter of the *Cisco Unified Communications Manager Administrative Guide*. **Note** If you enter a directory URI and also enter a directory number in the Primary Extension field, this directory URI automatically becomes the primary directory URI that is associated to that directory number.
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. **Tip** The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Unified CM does not require that you enter a user ID that already exists in the database.
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. Unified CM uses this locale for extension mobility and the Cisco Unified CM User Options. For Cisco Extension Mobility login, the locale that is specified takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Unified CM 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.

Field	Description
Associated PC	This required field applies for Cisco IP Softphone users.
Digest Credentials	Enter a string of alphanumeric characters. Unified CM 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 about digest authentication, see 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.
Service Settings	
Home Cluster	Check this check box if the end user is homed to this cluster. The end user should only be homed to one cluster within the enterprise. **Note** IM and Presence does not function properly if an end user is assigned to more than one home cluster.
Enable User for IM and Presence	Check this check box to enable the end user (on the home cluster) for IM and Presence. Configure IM and Presence in the associated service profile. **Note** You must install a Unified CM IM and Presence node along with this Unified CM cluster. Use the **User Management** > **User Settings** > **UC Services** menu to configure the IM and Presence service.
UC Service Profile	Choose a UC service profile from the drop-down list box. To view the settings for each UC service profile, click the More Details link.
Device Associations	
Controlled Devices	After you associate the device, this field displays the description information (for example, the MAC address) that the end user controls. This field appears after you create a user in the database. To associate a device with this end user, select the Device Association button. To associate a line appearance to this end user for presence, select the Line Appearance Association from Presence button. Doing so enables the on-the-phone status information to IM and Presence clients when this line appearance is off-hook. The Line Appearance choices presented depend on the lines associated with the controlled devices. **Note** If you want additional line appearance associations, or multiple user associations for a single line appearance, see the **Call Routing** > **Directory Number** window.
Available Profiles	This drop-down list box displays the device profiles that are available for association with this end user.

Field	Description
CTI Controlled Profiles	This drop-down list box displays the CTI controlled profiles that are available for association with an end user who is configured for CTI.
Extension Mobility **Note** Extension Mobility is not supported for third-party AS-SIP.	
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 appears 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 drop-down 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.
BLF Presence Group	Use this field to configure the BLF Presence feature. From the drop-down list box, choose a BLF presence group for the end user. The selected group specifies the destinations that the end user can monitor. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Unified CM Administration also appear in the drop-down list box. BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. See the *Cisco Unified Communications Manager Features and Services Guide*.
SUBSCRIBE Calling Search Space	Supported with the BLF Presence feature, the SUBSCRIBE calling search space determines how Unified CM 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 Unified CM Administration appear 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 box, 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.

Field	Description
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 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.
IPCC Extension	From the drop-down list box, choose an IPCC extension for this end user. **Note** This field appears only if the IPCC Express Installed enterprise parameter is set to True.
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) are 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.

Field	Description
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 DLUs appear 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 Unified CM Administration or remove the assignment after you enable Mobile Connect, two DLUs are 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 were 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.
Mutilevel Precedence and Preemption Authorization	
MLPP User Identification Number	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. **Note** The MLPP User Identification number must comprise 6 - 20 numeric characters. For information on how to configure the End User CAPF Profile, see the *Cisco Unified Communications Manager Security Guide*.

Field	Description
MLPP Password	Enter the MLPP password. **Note** The MLPP Password must comprise 4 - 20 numeric characters.
Confirm MLPP Password	Confirm the MLPP password. **Note** To confirm that you entered the MLPP Password correctly, re-enter the password in this field.
MLPP Precedence Authorization Level	Set the MLPP Precedence Authorization Level. The following precedence levels indicate the priority level that is associated with a call: • 0: Flash Override (highest) • 1: Flash • 2: Immediate • 3: Priority • 4: Routine (lowest) You can set the Precedence Authorization Level to any standard precedence level from Routine to Executive Override. Calls of equal or lower precedence are authorized to be originated by the user.

Related Topics

Associate devices to end user, on page 14

Create 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 (Unified CM) Administration.

Before You Begin

- You must configure Unified CM for voice messaging.
- You must configure the Cisco Unity Connection server to use the integrated mailbox feature. See the "Creating Multiple User Accounts from Unified CM 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 define an appropriate template and Class of Service (COS) for any voice-messaging users that you plan to add in Unified CM 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 appears in the Related Links menu.
- 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 about how to use the import feature, see the "Creating Multiple User Accounts from Unified CM 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 define a primary extension; otherwise, the Create Cisco Unity User link does not appear in the Related Links drop-down list box.

Step 3 From the Related Links drop-down list box, choose the Create Cisco Unity User link, and then click **Go**. The Add Cisco Unity User dialog box appears.

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 then 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 is 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 After you integrate the Cisco Unity Connection user with the Unified CM end user, you cannot edit fields in Cisco Unity Connection Administration such as Alias (User ID in Unified CM Administration), First Name, Last Name, and Extension (Primary Extension in Unified CM Administration). You can only update these fields in Unified CM Administration.

Related Topics

Change 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.

Related Topics

Change 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).

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

Step 4 Click Save.

Related Topics

Manage 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.

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 2: Application user and end user credential settings and fields, on page 12.

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

Related Topics

About end user setup, on page 1

Credential settings and fields

The following table describes the credential settings for end users and application users. These settings do not apply to application user or end user digest credentials.

Table 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.

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

Related Topics

Set up end user information

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 profiles you want to configure.
The End User Configuration window appears with information about the chosen end user.

Step 2 Click the user ID.

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 then click **Go**.
The Manager Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager Assistant with proxy line support and shared line support in the *Cisco Unified Communications Manager Features and Services Guide*.

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 then 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 then click **Go**.
The Assistant Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager Assistant with proxy line support and shared line support in the *Cisco Unified Communications Manager Features and Services Guide*.

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 then click **Go**.
The User Privilege window appears for this end user.

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 then click **Go**.

Related Topics

View user roles, access control groups, and permissions

Associate devices to end user

You can associate devices over which end users 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 (*) appears 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 appears, 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 appears.

Because you may have several devices in your network, Cisco Unified Communications Manager (Unified CM) 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, Unified CM Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Unified CM 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, on page 15.

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) 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 appear. You can change the number of items that appears 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 names.
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:

a) **Select All**: Click this button to select all devices that appear in this window.
b) **Clear All**—Click this button to uncheck the check boxes next to all devices that appear in this window.

c) **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.

d) **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.

e) **Save Selected/Changes**—Click this button to associate the devices that you selected with this end user.

f) **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 dialog box 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, choose Back to User, and then click **Go**.
The End User Configuration window appears, and the associated devices that you chose appear in the Controlled Devices pane.

Related Topics

Associate Cisco Extension Mobility profile to Cisco Unified IP Phone

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 sign 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 Unified Communications Manager Features and Services Guide*.

Related Topics