



## CHAPTER 20

# Application Users and End Users

---

The Application User Configuration window and the End User Configuration window in Cisco Unified Communications Manager Administration allow the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users and end users. This chapter describes the options for managing user information.

See “[Application User Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for more procedures on adding application users and configuring their application profiles.

See “[End User Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for procedures on managing and updating end user information.

This chapter includes the following topics:

- [Managing Application User and End User Configuration Checklist, page 20-1](#)
- [Application Users, page 20-2](#)
- [End Users, page 20-3](#)
- [Credential Management, page 20-4](#)
- [User and Application Profiles, page 20-5](#)
- [Device Association, page 20-5](#)
- [Cisco Unified Mobility for End Users, page 20-6](#)
- [Cisco Extension Mobility Profiles, page 20-7](#)
- [Cisco IP Softphone Profiles, page 20-7](#)
- [Where to Find More Information, page 20-7](#)

## Managing Application User and End User Configuration Checklist

The Application User Configuration window and the End User Configuration window in Cisco Unified Communications Manager Administration allow you to add, search, display, and maintain information about Cisco Unified Communications Manager application users and end users.

Table 20-1 lists the general steps and guidelines for managing application user and end user information. For more information, see the “Application Users” section on page 20-2, “End Users” section on page 20-3, and the “Where to Find More Information” section on page 20-7.

**Table 20-1 Application User and End User Configuration Checklist**

Configuration Steps		Related procedures and topics
<b>Step 1</b>	Search for an application user.	<a href="#">Application User Configuration Settings</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 2</b>	Add an application user as needed.	<a href="#">Application User Configuration Settings</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 3</b>	Manage application user credentials.	<a href="#">Managing Application User Credential Information</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 4</b>	Search for an end user.	<a href="#">End User Configuration Settings</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 5</b>	Add an end user as needed.	<a href="#">End User Configuration Settings</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 6</b>	Configure application profiles for end users.	<a href="#">Configuring User-Related Information for End Users</a> , <i>Cisco Unified Communications Manager Administration Guide</i>
<b>Step 7</b>	Manage end user credentials.	<a href="#">Managing End User Credential Information</a> , <i>Cisco Unified Communications Manager Administration Guide</i>

## Application Users

Application user configuration allows updates to the application users that are associated with Cisco Unified Communications Manager. By default, Cisco Unified Communications Manager Administration includes these application users:

- CCMAAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

Installation requires you to configure an administrator login and password for the system. You cannot delete these default application users or the administrator user that you create at install, but you can change their passwords and modify the lists of devices that they control.

**Tip**

Ensure that you do not lose the password that you created during installation.

**Note**

Administrator users in the Standard CCM Super Users group can access all administrative applications in the Cisco Unified Communications Manager Administration navigation menu (Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting) with a single sign-on to one of the applications.

You set the default Administrator username and password during Cisco Unified Communications Manager installation. You can change the administrator password or set up a new administrator account in the Application User Configuration window in Cisco Unified Communications Manager Administration.

To configure application user information in Cisco Unified Communications Manager, use the **User Management > Application User** menu option in Cisco Unified Communications Manager Administration.

**Note**

To configure this user for Cisco Unity or Cisco Unity Connection, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.

See [“Application User Configuration”](#) in the *Cisco Unified Communications Manager Administration Guide* for details.

## End Users

You can add end users to the Cisco Unified Communications Manager database, or you can use the corporate LDAP directory. If you use the corporate directory for authentication, end users use their LDAP directory passwords; you cannot change these passwords. You can, however, configure and change end user PINs.

**Note**

If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail. The system does not support empty (null) credentials. See [“Assigning and Configuring Credential Policy Defaults”](#) section on page 85-3 in the *Cisco Unified Communications Manager Administration Guide* for more information.

You can add new end users through Cisco Unified Communications Manager Administration only when synchronization with the corporate LDAP server is disabled. When synchronization is disabled, you can add new users, and you can change the settings of existing users, including the user ID. If synchronization is enabled, you cannot add users, delete users, or change existing user IDs. You can, however, change all other settings for existing end users in the End User Configuration window.

To check whether LDAP synchronization is enabled, choose **System > LDAP > LDAP System** in Cisco Unified Communications Manager Administration. If the Enable Synchronizing from LDAP Server check box is checked, you know that synchronization is enabled. See “[LDAP System Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for details.

To configure end user information, choose **User Management > End User** in Cisco Unified Communications Manager Administration. See “[End User Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for details.

You can use the End User, Phone, DN, and LA Configuration window to add a new user and a new phone at the same time. You can associate a directory number and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose **User Management > User/Phone Add**. See “[User/Phone Add Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for configuration details.

**Note**

The End User, Phone, DN, and LA Configuration window only allows adding a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

**Note**

To configure this user for Cisco Unity or Cisco Unity Connection, you configure the end user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration. See “[End User Configuration](#)” and “[User/Phone Add Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for more details.

## Credential Management

When you configure an application or end user, you can add or change login credentials (password or PIN) in the user configuration window.

After the user gets added to the database, you can manage these credentials in the Credential Configuration for window, which you access with the Edit Credentials button in the End User or Application User Configuration window. For example, you can block the user from changing the password, or you can require the user to change the password at the next login.

You can also view lockout events and reset a lockout for a password or PIN for the user. Authentication events get updated in the window according to the credential policy that you assigned to this user.

The Credential Configuration window also provides an option to change the user credential policy assignment. For more information about credential policies, see “[Credential Policy](#)” section on [page 21-1](#).

To manage credentials for individual users, see “[Managing Application User Credential Information](#)” and “[Managing End User Credential Information](#)” in the *Cisco Unified Communications Manager Administration Guide*.

# User and Application Profiles

After you add a new application or end user, you can assign a CAPF profile with the End User CAPF Profile or the Application User CAPF Profile menu options. Cisco Unified Communications Manager uses the CAPF profile to authenticate application or end user certificate downloads from the CAPF server. JTAPI / TSP or CTI applications use this certificate to establish a secure connection with Cisco CTIManager.

After you assign the profile, the CAPF Information pane in the user configuration window displays the assigned profile and allows you to update the settings. For general information about CAPF profiles, see the “[Application User CAPF Profile Configuration](#)” section and the “[End User CAPF Profile Configuration](#)” section of the *Cisco Unified Communications Manager Administration Guide*. For detailed information about CAPF profiles, see the *Cisco Unified Communications Manager Security Guide*.

After you add a new end user, options in the Extension Mobility pane allow you to configure extension mobility profiles. These profiles allow each end user to personalize Cisco Extension Mobility. For more information about extension mobility profiles, see the “[Cisco Extension Mobility](#)” chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

For information on configuring application profiles for end users, see the “[Configuring User-Related Information for End Users](#)” section of the *Cisco Unified Communications Manager Administration Guide*.

## Device Association

Associating devices to an application user or to an end user gives the user control over specified devices. Application users and end users control some devices, such as phones. When application users or end users have control of a phone, they can control certain settings, such as speed dial and call forwarding, for that phone. See the following topics for additional information about associating devices with users:

- [Device Association for Application Users, page 20-5](#)
- [Device Association for End Users, page 20-6](#)

## Device Association for Application Users

Use the Device Information portion of the Application User Configuration window to associate devices with an existing application user. The Available Devices pane lists the devices that are available for association with an application user. The Available Devices pane lists devices by device name. To search for additional devices to associate with an application user, use the **Find more Phones**, **Find more Route Points**, and **Find more Pilot Points** buttons. Each button opens a popup window where you can limit the list of devices by entering search criteria based on all or part of the device name, description, or other parameter. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name, description, or directory number.
- Choose the comparison operator, such as begins with.
- Enter search text.

For example, to list all extensions that begin with ‘5,’ you would choose Directory Number begins with and then enter **5** in the text box.

After you have specified the search criteria to display devices, all matching, available devices display in the Search Results. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the application user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

For more information on assigning devices to an application user, see [“Associating Devices to an Application User”](#) in the *Cisco Unified Communications Manager Administration Guide*.

## Device Association for End Users

Use the Device Associations portion of the End User Configuration window to associate devices with an existing end user. The Controlled Devices pane lists the devices that are already associated with an end user. The Controlled Devices pane lists devices by device name. To search for additional devices to associate with an end user, use the **Device Association** button. This button opens the User Device Association window where you can limit the list of devices by entering search criteria based on all or part of the device name or description. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name or description.
- Choose the comparison operator, such as begins with.
- Enter search text.

After you have specified the search criteria to display devices, all matching, available devices display in the Device association for (this end user) portion of the User Device Association window. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the end user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

For a detailed procedure for assigning devices to an end user, see [“Associating Devices to an End User”](#) in the *Cisco Unified Communications Manager Administration Guide*.

## Cisco Unified Mobility for End Users

In the End User Configuration window, you can enable Mobile Connect and Mobile Connect Access for the user. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units for Mobile Connect, and assigning a device to the user specifically for Cisco Unified Mobility controls the number of device license units that are consumed for Cisco Unified Mobility. For more information on how licensing works with Cisco Unified Mobility, see the [“Licenses for Cisco Unified Mobility”](#) section in the *Cisco Unified Communications Manager Features and Services Guide* and the [“Changing an End User Password”](#) section in the *Cisco Unified Communications Manager Administration Guide*.

In the End User Configuration window, you can also configure the maximum time that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to a desktop phone. Likewise, you can configure the maximum number of phones to which the user is permitted to transfer calls from the desktop phone.

The End User Configuration window lists the remote destination profiles that are configured for the end user. For more information on remote destination profiles, see “[Changing an End User Password](#)” in the *Cisco Unified Communications Manager Administration Guide* and “[Cisco Unified Mobility](#)” in the *Cisco Unified Communications Manager Features and Services Guide*.

## Cisco Extension Mobility Profiles

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

User device profiles and device profile defaults support the Cisco Extension Mobility feature. The user device profile includes the following information:

- Device Profile Information—Includes Device Type, User Device Profile Name, Description, User Hold Audio Source, and User Locale.
- Phone Button Information—Includes Phone Button Template for the device type.
- Softkey Template Information—Includes list of available softkey templates.
- Expansion Module Information—Includes Cisco Unified IP Phone add-on modules such as the Cisco Unified IP Phone 7914 Expansion Module.
- Multilevel Precedence and Preemption Information—Includes MLPP domain, indication, and preemption settings.
- Logged-Out Default Profile Information—Includes Log In User ID

An authentication scheme authenticates the user. The workflow engine sends an XML string through an HTTP post request to the Login Service. The string contains the following items:

- User name and password of the login application
- Device name that is based on the MAC address of the device on which the user wants their profile to reside

A dialog prompt displays on the device of the user.

For more information on Cisco Extension Mobility, see “[Cisco Extension Mobility](#)” in the *Cisco Unified Communications Manager Features and Services Guide*.

## Cisco IP Softphone Profiles

You can associate a device (line) to a user as a Cisco IP Softphone. This enables users to use their desktop PC to place and receive telephone calls and to control an IP telephone.

For more information on Cisco IP Softphone, see the *Cisco IP Softphone Administrator Guide*.

## Where to Find More Information

### Related Topics

- [Managing Application User and End User Configuration Checklist, page 20-1](#)

- [Application Users](#), page 20-2
- [End Users](#), page 20-3
- [Credential Management](#), page 20-4
- [User and Application Profiles](#), page 20-5
- [Device Association](#), page 20-5
- [Cisco Unified Mobility for End Users](#), page 20-6
- [Cisco Extension Mobility Profiles](#), page 20-7
- [Cisco IP Softphone Profiles](#), page 20-7
- [Application User Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [End User Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [User/Phone Add Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Cisco Unified IP Phone Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Credential Policy Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Credential Policy Default Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [LDAP System Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Cisco Unity Messaging Integration](#), page 31-1
- [Cisco Extension Mobility](#), *Cisco Unified Communications Manager Features and Services Guide*

**Additional Cisco Documentation**

- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*
- *Cisco IP Softphone Administrator Guide*
- *Cisco IP Softphone User Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified IP Phone user documentation and release notes (all models)