



## Preparing to Add User Accounts

---

Before you create Cisco Unity Connection user accounts—individually by using Cisco Unity Connection Administration, in bulk by using Cisco Unity Connection Bulk Administration Manager, or by using the Integrated Mailbox Configuration Tool—you need to make decisions about many of the settings that will be applied to the accounts as they are created.

See the following sections in this chapter for information that will help you prepare for creating user accounts:

- [Templates, page 2-1](#)
- [Class of Service, page 2-2](#)
- [Schedules, page 2-4](#)
- [Authentication Rules, page 2-4](#)
- [Roles, page 2-5](#)

## Templates

When you create user accounts in Cisco Unity Connection, each account is based on a user template. User templates contain settings that are applicable for most users of a particular type (such as a department). For example, if you are setting up accounts for the members of a sales department, you can set up message notifications, specify that messages left for the sales employees will be encrypted for extra security, increase the length of messages that callers can leave, and make changes to settings that control the Connection conversation that the sales employees hear.

If a particular setting must be unique for each user account, leave that setting blank on the user template, and plan to finish setting up the account by modifying it after it is created. User settings can be modified at any time.

It is important to note that changes to settings in a template do not affect any existing user accounts that were based on that template. After you create user accounts, you cannot use a template to modify them. Instead, you can:

- Customize user settings for individual accounts in Cisco Unity Connection Administration.
- Use Bulk Edit to modify user settings for multiple user accounts. For example, you might use this tool to change a setting so that a group of users will no longer be listed in the phone directory, or to associate a group of users with a particular phone system integration. Alternatively, you can use the Cisco Unity Connection Bulk Administration Manager to modify multiple user accounts. See the online Help for either tool for information on using the tool.

Users can also customize some of their own settings either by accessing the Cisco Unity Assistant or by using the Connection phone conversation.

## Cisco Unity Connection Default Templates

Cisco Unity Connection comes with the following predefined user templates, which you can modify but not delete:

<b>Voice Mail User Template</b>	The settings on this template are suitable for most users.
<b>Administrator Template</b>	The settings on this template are suitable for users who will administer Connection. User accounts that are based on this template do not have voice mailboxes.

For instructions on creating or modifying user templates, see the [“Adding, Modifying, or Deleting a User Template”](#) chapter.

## Class of Service

A class of service (COS) defines limits and permissions for using Cisco Unity Connection. For example, a COS:

- Controls access to features, such as Text to Speech e-mail or live reply.
- Controls how users interact with Connection. For example, a COS dictates the maximum length of user messages and greetings, whether users can choose to be listed in directory assistance, and whether users can send messages to a system distribution list.
- Specifies the restriction table used to control the phone numbers users can use for message notification, call transfer, and other tasks. See the [“Restriction Tables”](#) section on page 2-3 for additional information.

A COS is specified in each user template; thus, a user is assigned to the COS that is specified in the template upon which the user account is based.



### Note

A COS is not specified for either the individual accounts or templates for users without voice mailboxes (administrators). Settings on the Class of Service pages are applicable only to users with voice mailboxes. The permissions associated with administrator accounts are controlled by settings on the System Settings > Roles pages in Connection Administration.

You can modify the predefined classes of service, and you can create new ones. Changes to the settings in a COS affect not only new members, but also existing members of the COS. COS settings cannot be changed in individual user Connection accounts; however, a user can be reassigned to a different COS at any time. When a COS includes access to a feature that requires individual licenses, you can assign groups of users to the COS only if enough licenses are available.

You cannot delete a COS that has users assigned to it without first reassigning the users to another COS.

## Cisco Unity Connection Default Classes of Service

Cisco Unity Connection includes the following predefined classes of service, which you can modify but not delete:

<b>Voice Mail User COS</b>	Contains settings that are applicable to users. By default, this COS is associated with the default Voice Mail User template.
<b>System</b>	A COS that special default user accounts are members of. This COS is read-only and cannot be modified or deleted.

For instructions on creating or modifying classes of service, see the [“Adding, Modifying, or Deleting a Class of Service”](#) chapter.

## Restriction Tables

Restriction tables allow you to control which phone numbers users and administrators can use for:

- Transferring calls, including both the numbers users can enter for transferring their calls, and the numbers that unidentified callers can enter when using Caller system transfers.
- Recording and playback by phone from Cisco Unity Connection applications, when the phone is the designated recording and playback device in the Media Master. (The Media Master is available in Cisco Unity Connection Administration, the Cisco Unity Assistant, and the Cisco Unity Inbox.)
- Sending message notifications.

For example, you can specify that users have calls transferred only to internal extensions. Restriction tables are applied regardless of how a user or administrator accesses Connection. They do not affect the phone numbers that users can dial when they are not logged on to Connection.

Each class of service specifies for its members a restriction table for call transfers, one for message notification, and one for fax deliveries. (Note that fax-related features are not available in this release of Connection). The restriction table can be the same for all three, or different for each.

## Cisco Unity Connection Default Restriction Tables

Cisco Unity Connection comes with the following predefined restriction tables, which you can modify (including changing their names) but not delete. By default, each of these restriction tables prevents access to long distance phone numbers.

<b>Default Fax</b>	Restricts numbers for fax delivery. (Note that fax-related features are not available in this release of Connection).
<b>Default Outdial</b>	Restricts numbers for message notifications. Also restricts the user extensions that Connection dials when the phone is selected as the recording and playback device in the Media Master. (The Media Master is available in Cisco Unity Connection Administration, the Cisco Unity Assistant, and the Cisco Unity Inbox.)

<b>Default System Transfer</b>	Restricts numbers that can be used for Caller system transfers, which allow unidentified callers to transfer to a number that they specify. For example, callers may want to dial a lobby or conference room phone that is not associated with a Connection user. By default, the table does not allow Connection to dial any numbers.
<b>Default Transfer</b>	Restricts numbers for call transfers.

## Schedules

Schedules (and associated sets of holidays) affect the greetings that callers hear when they reach a user mailbox. The standard and closed user greetings play according to the days and times that you specify in a schedule; likewise, user holiday greetings play according to the dates and times you specify in the holiday schedule associated with a schedule.

Cisco Unity Connection offers two predefined schedules: All Hours and Weekdays, both of which can be modified. The default Voice Mail User template uses the Weekdays schedule, unless you select a different schedule. (By default, the Weekdays schedule is configured to observe standard hours from 8 a.m. through 5 p.m. Monday through Friday.) In addition, you can create up to 64 schedules for your organization to accommodate the standard working hours of different groups of employees.

For each schedule that you create or modify, you can identify multiple ranges of hours and days that make up the standard and closed hours, and associate a holiday schedule that defines specific holiday dates and times:

<b>Standard Hours</b>	The hours and days that make up the normal business hours, when the organization is open. Standard hours can include multiple time ranges and different time ranges on different days. (For example, standard hours for an organization might be Monday through Friday from 8 a.m. to 12 p.m. and 1 p.m. to 5 p.m., to accommodate a lunch break, and Saturday from 9 a.m. to 1 p.m.)
<b>Closed Hours</b>	The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.
<b>Holidays</b>	When a Holiday setting is in effect, Connection plays holiday greetings (if enabled). You can set up several years of holidays at a time. Because many holidays occur on different dates each year, confirm annually that the holiday schedule remains accurate.

## Authentication Rules

Authentication rules govern user passwords and account lockouts for all Cisco Unity Connection user accounts. You use authentication rules to secure how users access Connection by phone, and how users access Cisco Unity Connection Administration and the Cisco Personal Communications Assistant (PCA).

Password and account lockout policies are controlled by settings on the System Settings > Authentication Rules page in Connection Administration. An authentication rule is selected on the Password Settings page of each user template and user account page. For each authentication rule, you can control how Connection governs user access. For example, you can specify:

- The number of failed logon attempts that are allowed before an account is locked

- The number of minutes an account remains locked before it is reset
- Whether a locked account must be unlocked manually by an administrator
- The minimum length allowed for passwords
- The number of days before a password will expire

## Cisco Unity Connection Default Authentication Rules

Connection includes the following predefined authentication rules:

<b>Recommended Voice Mail Authentication Rule</b>	By default, Connection applies this rule to the Voice Mail password on the Password Settings page of each user account and user template for which you set up user access to Connection by phone.
<b>Recommended Web Application Authentication Rule</b>	By default, Connection applies this rule to the Web Application password on the Password Settings page of each user account and user template for which you set up user access to Cisco Unity Connection Administration, or to the Cisco Personal Communications Assistant.

You can change these defaults, and can create an unlimited number of additional authentication rules.

## Roles

The Cisco Unity Connection user accounts that are used to administer Connection have levels of privileges, set according to a list of predefined roles. Roles specify which tasks administrators can do in Connection Administration.

In the current version of Connection, you cannot make changes to the default permissions that are associated with each role. However, you can change which roles are assigned to an administrator at any time.

## Cisco Unity Connection Default Roles

Connection comes with the following predefined administrator roles:

<b>Audio Text Administrator</b>	Administers call handlers, directory handlers, and interview handlers.
<b>Greeting Administrator</b>	Manages call handler recorded greetings over the phone by allowing access to the Cisco Unity Greetings Administrator.  <b>Note</b> The Greeting Administrator is the only role that is not truly an administrative role, in that the Greeting Administrator does not have access to Connection Administration. Because the Greeting Administrator will instead require access to the Connection phone conversation in order to use the Cisco Unity Greetings Administrator, assign the Greeting Administrator role to a User with Voice Mailbox account.

<b>Help Desk Administrator</b>	Resets user passwords and unlocks user accounts; can view user setting pages.
<b>Technician</b>	Has access to all functions that enable management of the Connection server and phone system integration settings; can run all reports and use diagnostic tools; and can view all system and user settings pages.
<b>User Administrator</b>	Administers user accounts; has access to all user administration functions, can run user-related reports, and can use user administration tools.
<b>System Administrator</b>	This is the top-level administration account; has access to all administrative functions, including all user and system settings, all reports, and all administration and diagnostic tools. The default administrator account that the installer specified during initial setup of Connection is set to this role. A System Administrator is the only role that has permission to create administrative accounts.