



CHAPTER 22

Setting Up Features That Are Controlled by Subscriber or Subscriber Template Settings

See the following sections in this chapter:

- [Specifying Subscriber Account Settings, page 22-1](#)
- [Specifying Subscriber Passwords Settings, page 22-2](#)
- [Specifying Subscriber Call Transfer Settings, page 22-3](#)
- [Specifying Subscriber Greetings Settings, page 22-3](#)
- [Specifying Subscriber Caller Input Settings, page 22-4](#)
- [Specifying Subscriber Message Settings, page 22-5](#)
- [Enabling or Modifying MWI Settings, page 22-5](#)
- [Specifying Subscriber Alternate Extension Settings, page 22-6](#)
- [Partitioning Subscriber Accounts for Message Addressing by Phone, page 22-8](#)

Specifying Subscriber Account Settings

On an individual subscriber Account Settings page, you can use the account settings to check the account status for an individual subscriber (whether an account is locked or unlocked). Cisco Unity locks a subscriber account automatically when the Cisco Unity Account Status check box is checked on the Subscriber Template Account page for the template that was used to create the subscriber account.

Cisco Unity also locks a subscriber account when the subscriber reaches the limit of failed logon attempts specified in the account policy:

- When subscribers use the phone to access Cisco Unity, the number of failed logon attempts allowed is set on the Subscribers > Account Policy > Unity Account Lockout page.
- When subscribers use the Cisco Personal Communications Assistant (PCA) to access Cisco Unity, the number of failed logon attempts allowed is set on the System > Authentication page.
- When subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity, and the applications use the Integrated Windows authentication method (which is the default), the account policy that is specified for each Active Directory account determines the number of failed logon attempts that are allowed before the user account cannot be used to access Windows (and therefore, the Cisco Unity Administrator or the Status Monitor).

However, when subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity, and the applications use the Anonymous authentication method, the number of failed logon attempts allowed is set on the System > Authentication page.

You can use the account settings to lock individual subscriber accounts to prevent subscribers from using the phone or a Cisco Unity web application to access Cisco Unity, or to specify billing IDs specific to your organization.

On the Subscriber Template Account Settings page, you can lock or unlock subscriber accounts, and enter a billing ID.

Note that you cannot use the account settings to change the logon, password, or lockout policy for individual subscriber accounts. For information on setting up the account policy that applies when subscribers access to Cisco Unity by phone, see the “[Managing Account Policy Settings](#)” chapter.

Specifying Subscriber Passwords Settings

Phone password settings on individual subscriber accounts define whether subscribers are prompted to enter a password when they access their Cisco Unity mailboxes by phone, whether they can set their own phone passwords, and when they must change their passwords. In addition, when a subscriber forgets a password, you can use the phone password settings to reset the password. When more than one subscriber has access to the same account, you can set the password and not allow subscribers to change it.

Note that the phone password is separate from the password that a subscriber uses to log on to the Cisco Personal Communications Assistant (PCA). For more information, see the “[Securing and Changing Cisco PCA Passwords](#)” section on page 28-9.

Also see the “Password and Account Policy Management” chapter of the *Security Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

The password settings on the Subscriber Template Passwords page can govern how subscribers initially log on to Cisco Unity by phone and to Cisco Unity web applications.

Whether subscribers are assigned the phone and Active Directory password specified in the template depends on how their Cisco Unity accounts are created. As a best practice, subscribers should not be assigned the template passwords. Instead, each subscriber should be assigned unique phone and Active Directory passwords. To learn more, see the “[Ensuring That Subscribers Are Assigned Unique and Secure Phone Passwords](#)” section on page 21-6 and the “[Ensuring That Subscribers Are Assigned Unique and Secure Active Directory Passwords](#)” section on page 21-7.



Note

During installation, the installer was prompted to change the default phone and Active Directory passwords for the {Default Subscriber} template from 12345 and 12345678 respectively to passwords that are more secure. If your system was upgraded from an earlier version of Cisco Unity, the passwords may remain unchanged. As a security precaution, confirm that the default passwords have been replaced with passwords that are eight or more characters long and non-trivial.

Template password settings also define whether subscribers set their own phone passwords and when they must change their passwords. For information on specifying a password policy, see the “[Phone Password Restriction Settings](#)” section on page 9-1. For information on specifying the logon and lockout policy that applies when subscribers access the Cisco Unity web applications that use Anonymous authentication, see the “[Authentication Settings](#)” section on page 11-1.

Specifying Subscriber Call Transfer Settings

Call transfer settings specify how Cisco Unity handles calls transferred from the automated attendant or a directory handler to subscriber phones. (Note that transfer options do not apply when an outside caller or another subscriber dials a subscriber extension directly.)

These settings also specify how Cisco Unity handles a transfer: Cisco Unity can either release the call to the phone system, or it can supervise the transfer. When Cisco Unity is set to supervise transfers, it can provide additional call control with call holding and call screening for indirect calls:

- With call holding, when the phone is busy, Cisco Unity can ask callers to hold. Each caller on hold uses a Cisco Unity port and a phone system port, so the total number of callers that can be holding in the queue at one time is limited by the number of available ports.

The wait time in the call holding queue for the first caller in the queue defaults to 25 seconds. If the caller is still on hold after this amount of time, Cisco Unity asks if the caller wants to continue holding, leave a message, or try another extension. If the caller does not press 1 to continue holding, or press 2 to leave a message, the caller will be transferred back to the Opening Greeting. Subsequent callers in the holding queue will be told how many other callers are in the queue ahead of them, in addition to these options. (For more information on call holding, see the [“Configuring Call Waiting Hold Time”](#) section on page 15-6 and the [“Working With Cisco Unity Music on Hold”](#) section on page 11-5.)

If call holding is not selected, callers are sent to whichever subscriber or handler greeting is enabled—the busy, standard, closed, or alternate greeting.

- With call screening, Cisco Unity can ask for the name of the caller before connecting to a subscriber. The subscriber can then hear who is calling and, when a phone is shared by more than one subscriber, who the call is for. The subscriber can then accept or refuse the call.

If the call is accepted, it is transferred to the subscriber phone. If the call is refused, Cisco Unity plays the applicable subscriber greeting.



Tip

See your phone system documentation for information on transfer, screening, and holding options for direct calls to subscriber extensions. Subscriber desk phones may also offer similar features.

Both primary and alternate extensions use the same transfer settings.

Subscribers have three transfer rules that you can customize: one for standard hours and one for closed hours of the active schedule, and an alternate transfer rule that, when enabled, overrides the standard and closed transfer rules and is in effect at all times. By default the alternate rule is enabled so a subscriber's transfer behavior is always the same unless configuration changes are made.

Specifying Subscriber Greetings Settings

Each subscriber account can have up to five greetings. The greeting settings specify which greetings are enabled, how long they are enabled, the greeting source, and the actions that Cisco Unity takes during and after each greeting. When a greeting is enabled, Cisco Unity will play the greeting in the applicable situation until the specified date and time arrives, and then the greeting is automatically disabled. A greeting can also be enabled to play indefinitely, which is useful for busy or closed greetings, or when an alternate greeting is used by a subscriber during a leave of absence.

Cisco Unity plays the greetings that you enable, as described in the following table. Note that some greetings override other greetings when they are enabled.

Standard	Plays at all times unless overridden by another greeting. You cannot disable the standard greeting.
Closed	Plays during the closed (nonbusiness) hours defined for the active schedule. A closed greeting overrides the standard greeting, and thus limits the standard greeting to the open hours defined for the active schedule.
Internal	Plays to internal callers only. It can provide information that only coworkers need to know. (For example, “I will be in the lab all afternoon.”) An internal greeting overrides the standard and closed greetings. Not all phone system integrations provide the support necessary for an internal greeting.
Busy	Plays when the extension is busy. (For example, “All of our operators are with other customers.”) A busy greeting overrides the standard, closed, and internal greetings. Not all phone system integrations provide the support necessary for a busy greeting.
Alternate	Can be used for a variety of special situations, such as vacations, leave of absence, or a holiday. (For example, “I will be out of the office until....”) An alternate greeting overrides all other greetings. You can customize how Cisco Unity behaves when a subscriber enables the alternate greeting. You can specify that Cisco Unity: <ul style="list-style-type: none"> • Plays a prompt to remind subscribers that the alternate greeting is enabled when they log on to Cisco Unity by phone. • Transfers callers directly to the alternate greeting without ringing the subscriber phone. • Prevents callers from skipping the greeting. • Prevents callers from leaving messages. • Sends a notice to subscribers after they send, reply to, or forward messages to other subscribers who have their alternate greeting enabled. By default, none of the above options are enabled and not all can be enabled on the Subscriber Template > Greetings page. To learn more, see the “Specifying How Cisco Unity Behaves When Subscribers Have Their Alternate Greeting Enabled” section on page 17-16.

Subscribers can enable as many greetings as they want; they can (re)record and manage all of their greetings by phone, or by using the Cisco Unity Assistant. Based on the options you select in the Cisco Unity Administrator, the Cisco Unity Assistant presents information to subscribers that explains how Cisco Unity handles their calls when their alternate greeting is enabled.

Specifying Subscriber Caller Input Settings

Caller input settings define actions that Cisco Unity takes in response to touchtone keys pressed by callers. For each subscriber greeting that allows caller input, you can use caller input settings to allow callers to skip the subscriber greeting, to record a message, to exit the greeting, or perhaps to transfer to a call handler, directory handler, or interview handler of your choice. (For Cisco Unity to recognize caller input during a subscriber greeting, the Allow Caller Input check box must be checked on each applicable Greetings page.)

Subscribers cannot enable caller input for a greeting, nor can they specify what Cisco Unity does when callers press specific keys; however, the greeting that mentions the key presses that are available to callers is recorded either by the subscriber or the administrator. (For example, “I am unable to take your call right now. To speak to my assistant, press 3. To leave a message, press 4. To speak to a sales representative, press 5.”)

You also use caller input settings to specify which key(s) subscribers can press to interrupt a subscriber greeting so that they can log on to Cisco Unity, and what subscribers hear after Cisco Unity prompts them to log on. For details and best practices, see the [“Logging On to Cisco Unity From Subscriber Greetings” section on page 17-10](#). For information on setting up system transfers, see the [“Setting Up System Transfers” section on page 15-11](#).

Use the following procedure to specify caller input settings.

To Specify Caller Input Settings on a Subscriber Template

-
- | | |
|---------------|---|
| Step 1 | In the Cisco Unity Administrator, go to any Subscribers > Subscriber Template > Caller Input page. |
| Step 2 | Select a key from the Caller Input Map or from the keypad. |
| Step 3 | Select an action. |
| Step 4 | Indicate whether to lock the key to that action. |
-

Specifying Subscriber Message Settings

Message settings define the following:

- The maximum recording length for messages left by unidentified callers. (Note that for some integrations, you can set up Cisco Unity so that when a caller records a message, a warning tone is played before the caller reaches the maximum allowable message length. See the [“Enabling a Warning Tone for End of Recording” section on page 15-8](#) for details.)
- What unidentified callers can do when leaving messages.
- The language of the Cisco Unity prompts that callers hear when leaving messages for subscribers.
- Whether subscribers are notified with message waiting indicators (MWIs) that they have voice messages.
- One or more extensions where the MWI will be activated when subscribers have voice messages.

Enabling or Modifying MWI Settings

Cisco Unity can use the MWI on the phone to alert the subscriber to new voice messages. MWIs are not used to indicate the receipt of new e-mail, fax, or return receipt messages.

To Enable MWIs

-
- | | |
|---------------|--|
| Step 1 | In the Cisco Unity Administrator, go to the applicable Subscribers > Subscribers > Messages page. |
| Step 2 | Confirm that the Use MWI for Message Notification check box is checked. |

- Step 3** Click the **Add** button located beneath the MWI Extensions table to add a row to the table. By default, the first row in the table contains an “X” to indicate the primary extension assigned to a subscriber. If you want one more extension and do not need to activate the MWI on the primary extension, you can also modify the first row.
- Step 4** Enter the applicable extension in the Extension field of the table. MWIs are automatically enabled for all rows in the table. When entering characters in the MWI Extensions table, consider the following:
- Enter digits **0** through **9**. Do not use spaces, dashes, or parentheses.
 - Enter **,** (comma) to insert a one-second pause.
 - Enter **#** and ***** to correspond to the # and * keys on the phone.
- Step 5** Click the **Save** icon.
- Step 6** Repeat [Step 3](#) through [Step 5](#) as necessary.
-

To Modify or Delete Alternate MWIs

- Step 1** In the Cisco Unity Administrator, go to the applicable **Subscribers > Subscribers > Messages** page.
- Step 2** Do either of the following:
- To modify an extension, change the extension in the MWI Extensions table.
 - To delete extensions, check the check boxes next to the rows that you want to delete in the MWI Extensions table, and then click the **Delete** button.
- Step 3** Click the **Save** icon.
- Step 4** Repeat [Step 2](#) and [Step 3](#) as necessary.
-

Specifying Subscriber Alternate Extension Settings

In addition to the primary extension that you specify for subscribers, you can assign subscribers up to nine alternate extensions. (The primary extension is the one that you assign to each subscriber when you create his or her subscriber account; it is listed on the Subscribers > Subscribers > Profile page.)

Reasons to Use Alternate Extensions

There are several reasons that you may want to specify alternate extensions for subscribers. For example, if you have more than one Cisco Unity server that accesses a single, corporate-wide directory, you may want to use alternate extensions to simplify addressing messages to subscribers at the different locations. With alternate extensions, the number that a subscriber uses when addressing a message to someone at another location can be the same number that the subscriber dials when calling. You may also want to use alternate extensions to:

- Handle multiple line appearances on subscriber phones.

- Offer easy message access on direct calls from a cell phone, home phone, or phone at an alternate work site (assuming that the phone number is passed along to Cisco Unity from these other phone systems). In addition, when such phones are used as alternate extensions, and are set to forward to Cisco Unity, callers can listen to the subscriber greeting, and leave messages for the subscriber just as they would when dialing the primary extension for the subscriber.

**Tip**

To reduce the number of requests from subscribers who want alternate extensions set up for multiple cell phones, home phones, and other phones, give subscribers class of service (COS) rights to specify their own set of alternate extensions. (See the Subscribers > Class of Service > Profile page.) With proper COS rights, a subscriber can specify up to five alternate extensions in the Cisco Unity Assistant—in addition to the nine that you can specify on the Subscribers > Alternate Extensions page in the Cisco Unity Administrator.

- Enable URL-based extensions in Cisco Unity for an integration with a SIP phone system.

How Alternate Extensions Work

Before you set up alternate extensions, review the following list for information on how alternate extensions work:

- Alternate extensions cannot exceed 30 characters in length. By default, each administrator-defined alternate extension must be at least 3 characters in length, while subscriber-defined alternate extensions must be at least 10 characters.

You can use the Advanced Settings tool in Tools Depot to specify a minimum extension length for the extensions entered in the Cisco Unity Administrator and the Cisco Unity Assistant. See the Advanced Settings Tool Help for details on using the settings. Respectively, the settings are Administration—Set the Minimum Length for Locations, and Administration—Set the Minimum Length for Subscriber-Defined Alternate Extensions.

- You can control whether subscribers can use the Cisco Unity Assistant to view the alternate extensions that you specify in the Cisco Unity Administrator. See the Subscribers > Class of Service > Profile page. The Subscriber-Defined Alternate Extension table displays the alternate extensions that the subscriber adds.
- Neither the Cisco Unity Administrator nor the Cisco Unity Assistant will accept an extension that is already assigned to another subscriber (either as a primary or alternate extension), or to a public distribution list, call handler, directory handler, or interview handler. Cisco Unity verifies that each alternate extension is unique—up to the dialing domain level, if applicable—before allowing either an administrator or a subscriber to create it.
- All alternate extensions use the same transfer settings as the primary extension.
- In many cases, Cisco Unity can activate a message waiting indicator (MWI) for an alternate extension. However, depending on the phones and phone systems involved, some additional phone system programming may be required to set this up.

Setting Up Alternate Extensions

Do the applicable procedure to add, modify, or delete alternate extensions:

- [To Add Administrator-Defined Alternate Extensions, page 22-8](#)
- [To Modify or Delete Alternate Extension\(s\), page 22-8](#)

To Add Administrator-Defined Alternate Extensions

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Alternate Extensions** page.
- Step 2** In the Administrator-Defined Alternate Extensions table, enter an extension in any row. When entering characters in the Alternate Extensions table, consider the following:
- You can enter an extension up to 30 characters in length. (SIP integrations can use up to 30 alphanumeric characters.)
 - Each extension must be unique—up to the dialing domain level, if applicable.
 - Enter digits **0** through **9**. Do not use spaces, dashes, or parentheses.
 - For SIP integrations, you can also enter a valid alias for a SIP URL. For example, if the URL is SIP:aabade@cisco.com, enter aabade. Do not use spaces.
 - Rows are numbered as a convenience. You can enter alternate extensions in any order, and you can have blank rows.
- Step 3** Repeat [Step 2](#) as necessary.
- Step 4** Click the **Save** icon. Alternate extensions are enabled for all rows in the table.
-

To Modify or Delete Alternate Extension(s)

- Step 1** In the Cisco Unity Administrator, go to any **Subscribers > Alternate Extensions** page.
- Step 2** Do any of the following:
- To modify an extension, change the extension in the Alternate Extensions table.
 - To delete extensions, check the check boxes next to the alternate extensions that you want to delete.
 - To remove all alternate extensions listed in the table, click **Select All**.
- Step 3** Click the **Save** icon.
- Step 4** Repeat [Step 2](#) and [Step 3](#) as necessary.
-



Note

You can run the Cisco Unity Bulk Import wizard when you want to add alternate extensions for multiple subscribers at once. When you do, the Cisco Unity Bulk Import wizard appends the new alternate extensions to the existing table of alternate extensions, beginning with the first blank row.

Partitioning Subscriber Accounts for Message Addressing by Phone

Cisco Unity allows you to partition subscriber accounts into separate groups to restrict who they can address messages to and who they can add to distribution lists, when they do so by phone.

To partition accounts, you define message addressing search scopes by associating subscribers with directory handlers.

By default, search scopes are defined for the system by the addressing option settings for the primary location that is configured for the Cisco Unity server. The option settings allow you to restrict message addressing to the global directory (all subscribers), to all subscribers in a dialing domain, or to all subscribers on the local Cisco Unity server.

When you associate subscribers with directory handlers, you can have Cisco Unity restrict their message addressing search scopes to the search option that is selected for the directory handler. The search option specified can be a dialing domain, the local Cisco Unity server, a location, a class of service or a public distribution list.

This can be useful for setting up a multi-tenant system where there is a need to prevent subscribers in one group from sending messages to subscribers in another group.

For example, if your organization needs to partition subscriber accounts into two groups such that subscribers in each group cannot address messages to subscribers in the other group, do the following tasks in order:

1. Create a separate class of service for each group.
2. Create a separate directory handler for each group for which the Search In options are set to a different one of the two classes of service that you created in task 1.
3. Create separate subscriber templates, and associate each template with a different one of the two directory handlers that you created in task 2.
4. Use the two templates to create the two groups of subscribers.

**Note**

Changes to settings in a template do not affect any existing subscriber accounts that were based on that template. After you create subscribers, you cannot use a template to modify them.

Alternatively, if the subscriber accounts already exist and are members of separate public distribution lists, you can associate a different directory handler with each distribution list, then use the Bulk Edit utility to associate each group of subscribers with the applicable directory handler.

Use the following procedure to associate subscribers with directory handlers.

To Associate a Subscriber or a Subscriber Template with a Directory Handler

- Step 1** In Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page or the **Subscribers > Template > Profile** page, as applicable.
- Step 2** Click **Limit Access To**, and click **Select**.
- Step 3** In the Directory Handler Selection dialog, search for the directory handler with which to associate the subscriber, and then double-click it.
- Step 4** Click the **Save** icon.

To modify subscriber search scopes, you can use either the Cisco Unity Administrator or Bulk Edit:

- To do so for an individual subscriber or for a subscriber template by using Cisco Unity Administrator, do the procedure [“To Associate a Subscriber or a Subscriber Template with a Directory Handler”](#) and select the new directory handler in [Step 3](#).
- To do so for a group of existing subscribers at once by using the Bulk Edit utility, see the Bulk Edit utility Help. The Bulk Edit utility is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop.)

