System Administration Guide for Cisco Unity (With Microsoft Exchange)

Release 5.x
Revised September 29, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13846-01

System Administration Guide for Cisco Unity Release 5.x (With Microsoft Exchange)

CONTENTS

Preface

This preface describes the purpose, audience, and conventions of the *System Administration Guide for Cisco Unity*, and provides information on how to obtain related documentation.

Purpose

The *System Administration Guide for Cisco Unity* introduces you to the Cisco Unity Administrator, which is the administration interface for Cisco Unity, and explains how to configure Cisco Unity.

The *System Administration Guide for Cisco Unity* focuses on Cisco Unity. It does not provide information on Microsoft Exchange, Microsoft Windows, IBM Lotus Domino, or setting up the Cisco Unity server as an e-mail server.

Audience

This guide is intended for system administrators and others who are responsible for managing Cisco Unity. If you are administering the Cisco Unity server, you need a working knowledge of Windows and of the message store (IBM Lotus Domino or Microsoft Exchange) in which voice messages are stored. Although knowledge of other voice messaging systems is useful, it is not required.

Document Conventions

This guide uses the following conventions:

Table 1 System Administration Guide for Cisco Unity Conventions

Convention	Descriptions
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Click **OK**.) • Information that you enter. (Example: Enter **Administrator** in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping <IP address>**.)

Table 1 System Administration Guide for Cisco Unity Conventions (continued)

Convention	Descriptions
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
>* (right angle bracket)	A right angle bracket is used to separate selections that you make: • On menus. (Example: On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.) • In the navigation bar of the Cisco Unity Administrator. (Example: Go to the **System > Configuration > Settings** page.)

The *System Administration Guide for Cisco Unity* also uses the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Cisco Unity Documentation

For descriptions and the URLs of Cisco Unity documentation on Cisco.com, see the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors

and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance, contact us by sending e-mail to export@cisco.com.

CHAPTER 1

Accessing and Using the Cisco Unity Administrator

See the following sections in this chapter:

Exiting and Starting the Cisco Unity Software

The following sections provide instructions on exiting the Cisco Unity software, shutting down and restarting the Cisco Unity server, and starting the Cisco Unity software.

Note For details on the accounts that you use to log on to the Cisco Unity server and the Cisco Unity Status Monitor, see the "About the Accounts That Can Be Used to Administer Cisco Unity" section on page 2-1.

Exiting the Cisco Unity Software

This section contains two procedures for exiting the Cisco Unity software: from the Cisco Unity server and from another computer.

Caution Do not use Kill av*.* to exit the Cisco Unity software. Kill av*.* does not stop all Cisco Unity services, and may cause problems with upgrades from Cisco Unity version 2.x.

Do not stop AvCsMgr by using the Services window or the Component Services window as a method to exit the Cisco Unity software. Stopping the AvCsMgr does not stop all Cisco Unity services and may cause unexpected results.

To Exit the Cisco Unity Software from the Cisco Unity Server

Step 1 If the system uses the automated attendant, route all calls to the operator.

Step 2 On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.

Step 3 Right-click the Cisco Unity icon in the status area of the taskbar.

(If the Cisco Unity icon is not in the taskbar, browse to the CommServer directory, and double-click **AvCsTrayStatus.exe**.)

Step 4 Click **Stop Cisco Unity**.

Step 5 Click **OK** to confirm that you want to exit the Cisco Unity software. Cisco Unity stops running when all calls are finished, and an "X" appears in the Cisco Unity icon.

Step 6 Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.

To Exit the Cisco Unity Software from Another Computer

Step 1 If the system uses the automated attendant, route all calls to the operator.

Step 2 If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to Step 3.

When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following sub-steps to access the Status Monitor:

a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.

b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.

c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or the Windows domain account.

d. Skip to Step 5.

Step 3 When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:

a. Log on to Windows by using any domain account that has the right to log on locally.

b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.

Step 4 On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.

Step 5 In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:

- Cisco Unity stops running after all calls are finished.
- Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.

Step 6 Click **Shut Down**.

Shutting Down or Restarting the Cisco Unity Server

Note Restarting the Cisco Unity server may result in delayed message notification and message waiting indication until MAPI logon to all subscriber mailboxes has been completed. Depending on the size of the subscriber database, it could take several hours to complete the MAPI logon.

If the Cisco Unity system has an expansion chassis or is set up for failover, note the following considerations before shutting down or restarting the Cisco Unity server:

Expansion chassis connected to the Cisco Unity server	When both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.
Cisco Unity failover	• When both servers are running and the active server is shut down, the inactive server becomes active. • When neither server is running, the first server started becomes the active server. • When the secondary server is active and configured for automatic failback, and the primary server is also running, the secondary server attempts failback on the failback schedule.

To Shut Down or Restart the Cisco Unity Server

Step 1 Exit the Cisco Unity software, if it is running, by using one of the procedures in the "Exiting the Cisco Unity Software" section on page 1-1.

Step 2 On the Windows Start menu, click **Shut Down**.

Step 3 Click **Shut Down or Restart**. During a restart, the Cisco Unity software starts automatically.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.

When Cisco Unity does not start successfully, two tones play and an "X" appears in the Cisco Unity icon in the status area of the taskbar.

Starting the Cisco Unity Software

This section contains two procedures for starting the Cisco Unity software: from the Cisco Unity server and from another computer.

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the procedures in this section only if you exited the Cisco Unity software and did not restart the server.

Exchange must be running before you start the Cisco Unity software—either on the partner Exchange server or on the Cisco Unity server, depending on your configuration.

If Exchange stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

To Start the Cisco Unity Software from the Cisco Unity Server

Step 1 On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.

Step 2 Right-click the Cisco Unity icon in the status area of the taskbar.

(If the Cisco Unity icon is not in the taskbar, browse to the CommServer directory, and double-click **AvCsTrayStatus.exe**.)

Step 3 Click **Start Cisco Unity**.

When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.

When Cisco Unity does not start successfully, two tones play and an "X" appears in the Cisco Unity icon.

Step 4 Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.

Step 5 If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.

To Start the Cisco Unity Software from Another Computer

Step 1 If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to Step 2.

When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:

a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.

b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.

c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account.

d. Skip to Step 4.

Step 2 When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:

a. Log on to Windows by using any domain account that has the right to log on locally.

b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.

Step 3 On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.

Step 4 In the Cisco Unity Status Monitor, click the System Status icon (the first icon), at the top of the page.

Step 5 Click **Start**.

Step 6 If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.

Accessing and Using the Cisco Unity Administrator

The Cisco Unity Administrator is a website that you use to do most administrative tasks. Administrative tasks include determining system schedules, specifying settings for individual subscribers (or for a group of subscribers by using a subscriber template), and implementing a call management plan.

See the following sections:

We welcome your feedback about Cisco Unity. To facilitate collecting feedback about Cisco Unity, the Cisco Unity Administrator includes a Feedback link from the navigation pane on the left side of the Cisco Unity Administrator. Click Feedback, and in the form that opens, enter any information that you want to send to us, then click Submit.

Accessing and Exiting the Cisco Unity Administrator

See the following sections:

Logging On to the Cisco Unity Administrator

Although the way in which you log on to the Cisco Unity Administrator depends on the type of authentication that it uses, the account that you use to log on remains the same: you can use either the administration account that was selected when Cisco Unity was installed, or you can use an applicable Active Directory account. For information on which accounts can be used to access the Cisco Unity Administrator, see the "About the Accounts That Can Be Used to Administer Cisco Unity" section on page 2-1.

Note Until you create a Cisco Unity subscriber account for the purpose of administering Cisco Unity, you must use the Active Directory credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

To log on to the Cisco Unity Administrator, use the applicable procedure in this section. Note that Cisco Unity does not permit more than 50 administrators to access the Cisco Unity Administrator at the same time.

To Log On to the Cisco Unity Administrator When It Uses Integrated Windows Authentication

Step 1 Log on to Windows on the Cisco Unity server (or a remote computer) by using either the administration account that was selected when Cisco Unity was installed, or an applicable Active Directory account.

Step 2 If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the Cisco Unity icon in the status area of the taskbar, and click **Launch System Admin**.

If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.

Step 3 If Internet Explorer prompts you, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed, or an applicable Active Directory account.

To Log On to the Cisco Unity Administrator When It Uses Anonymous Authentication

Step 1 Log on to Windows on the Cisco Unity server (or a remote computer) by using any Active Directory account that has the right to log on locally.

Step 2 If you logged on to the Cisco Unity Administrator on the Cisco Unity server, right-click the Cisco Unity icon in the status area of the taskbar, and click **Launch System Admin**.

If you logged on to the Cisco Unity Administrator on a computer other than the Cisco Unity server, start Internet Explorer, and go to **http://<Cisco Unity server name>/web/sa**.

Step 3 On the Cisco Unity Log On page, enter either the user name, password, and domain for the administration account that was selected when Cisco Unity was installed, or enter the user name, password, and domain for an applicable Active Directory account, and click **Log On**.

You can use the settings on the Authentication page in the Cisco Unity Administrator to specify whether the Log On offers the following options:

- Remember User Name
- Remember Password
- Remember Domain

When you specify that Cisco Unity will remember your user name, password, or domain, you will not have to enter them the next time that you log on. Instead, the fields are automatically populated in the Log On page.

Exiting the Cisco Unity Administrator

To Exit the Cisco Unity Administrator

Step 1 Click the **Log Off** button on the lower left area of the Cisco Unity Administrator page.

Step 2 Exit **Internet Explorer**.

Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator

Each Cisco Unity Administrator provides links to the Cisco Unity Administrator websites on other networked Cisco Unity servers. By clicking the links, you can access subscriber accounts and other Cisco Unity objects on another Cisco Unity server simply by browsing to the Cisco Unity Administrator on the Cisco Unity server on which those accounts and objects were created.

When you want to find a subscriber account, but do not know on which Cisco Unity server in the network the account was created, you can search for it from any subscriber page in the Cisco Unity Administrator on your local Cisco Unity server by using the Find icon.

When the Cisco Unity Administrator uses the Integrated Windows authentication method, you are not required to re-enter your Active Directory account credentials when you browse to another Cisco Unity Administrator website from your local Cisco Unity server. Note that this is true only if you log on to the Cisco Unity Administrator on your local server by using the credentials of the Active Directory account that is associated with a Cisco Unity subscriber account that has appropriate class of service (COS) rights on the remote Cisco Unity server.

However, when the Cisco Unity Administrator uses the Anonymous authentication method, you are prompted to enter authentication credentials regardless of the account you used to log on to the Cisco Unity Administrator on your local server. In this case, simply enter the applicable credentials for the Cisco Unity Administrator website that you want to access.

To Browse to Another Cisco Unity Administrator on a Networked Cisco Unity Server

Step 1 Near the bottom of the navigation bar on the left side of the Cisco Unity Administrator interface, click **Unity Servers**. The Server Chooser page appears.

Step 2 From the list, click the server that you want to access.

Step 3 If prompted, enter the applicable credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server that you selected.

Do the following procedure to use the Cisco Unity Administrator on your local Cisco Unity server to search for subscriber accounts on other Cisco Unity servers in the network.

To Search for Subscriber Accounts Created on a Cisco Unity Server Other than Your Local Cisco Unity Server

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers page**.

Step 2 Click the **Find** icon.

Step 3 Indicate whether to search by alias, extension, first name, or last name.

Step 4 Enter the applicable alias, extension, or name. You also can enter * to display a list of all subscribers, or enter one or more characters or values followed by * to narrow your search.

Step 5 Check the **Search All Cisco Unity Servers** check box.

Step 6 Click **Find**.

Step 7 On the list of matches, click the name of the subscriber to display the record.

Step 8 If prompted, enter the applicable credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server on which the subscriber account was created. The subscriber profile page is displayed in the new browser window.

Cisco Unity Administrator User Interface

The Cisco Unity Administrator interface is divided into three areas.

Navigation bar	Located along the left side of the interface; contains links to categories of data pages.
Page	Where Cisco Unity data is entered and displayed. The page name is highlighted at the top of the page.
Title bar	Displays the name of the record or of the group of settings that appears on the page. The title bar also features command icons that initiate actions such as saving and finding records.

See the following sections for additional details:

- Cisco Unity Data, page 1-8
- Navigation, page 1-9
- Command Icons, page 1-9
- About the Media Master, page 1-10

Cisco Unity Data

The Cisco Unity Administrator features links from the main navigation bar to five groupings of data, representing subscribers and other Cisco Unity entities.

The data groupings available from the Cisco Unity Administrator include:

Subscribers

These pages are used to enter data related to individual subscriber records. Also included are subscriber template pages, which contain settings that are applied to groups of subscribers. Settings include schedules, passwords, account permissions, call processing and transfer options, and distribution lists.

Call Management

These pages are used to set how Cisco Unity answers, routes, transfers, and records calls. Settings include call routing, prerecorded caller interviews, call recording, and allowing or blocking certain dial strings.

Reports

These pages are used to generate reports on subscriber-based and system-based data. Reports can be generated for any of the data stored in the system, such as subscriber message activity, distribution lists, phone logons, disk storage, administration access, and port usage.

Network

These pages are used to add and view information about other Cisco Unity locations and to specify AMIS, VPIM, and/or Cisco Unity Bridge settings. Note that the network data pages are available only when Digital Networking, AMIS, VPIM, and/or the Cisco Unity Bridge are installed.

System

These pages are used to customize and view numerous system features, including business schedules, annual holidays, recording settings, and languages.

Navigation

There are two levels of navigation in the Cisco Unity Administrator.

- At the first level, the navigation bar displays the data categories and provides links to each group of pages within those categories.
- At the second level, the navigation bar provides a link to each page within a selected group. When a page is displayed, you can access individual records of that page type by clicking the Find icon. For more information, see the "Finding Records" section on page 1-11.

Always use the Cisco Unity navigation bar, rather than the Internet Explorer navigation buttons, to move between pages. Otherwise, incorrect data may be displayed.

Command Icons

The command icons are located in the title bar, which is in the upper-right area of each Cisco Unity Administrator page.

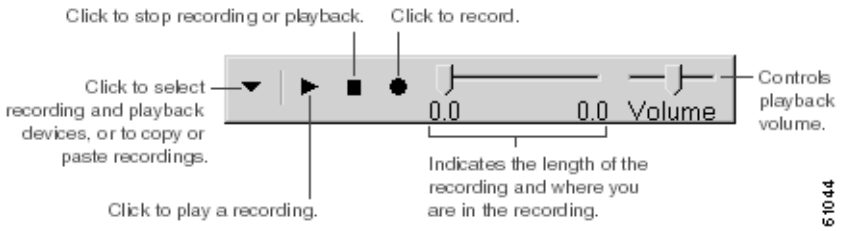
	Save icon	Saves data that you have entered. Available only when you have changed the record.
	Find icon	Opens the Find window, where you search for existing records in the displayed category.
	Add icon	Opens the Add window, where you enter information to create a new record in the displayed category.
	Delete icon	Deletes the displayed record.
	Run icon	Generates a report. Available only on Reports pages.

	Online Documentation icon	Provides in-depth descriptions and conceptual Help and includes an index and glossary.
	Field Help icon	Displays question marks next to fields and buttons for which Help is available.

About the Media Master

The Media Master control bar appears on each page of the Cisco Unity Administrator where recordings can be made. See Figure 1-1. The first time that you access a Cisco Unity Administrator page that contains the Media Master, you are prompted to install it. The Media Master installs automatically as long as you have local administrative rights to the Cisco Unity server. On subsequent visits to web pages that contain the Media Master, it is created from the locally installed copy.

Figure 1-1 Media Master Control Bar



To learn how to use the Media Master and other Cisco Unity tools to make and play recordings, see the "Recording Greetings and Names" chapter.

Using Help

The Cisco Unity Administrator includes two types of context-sensitive Help:

Online Documentation	Displays Help for the current page in the Cisco Unity Administrator, and links to additional topics.
Field Help	Displays descriptions of individual fields in the Cisco Unity Administrator.

An FAQ that addresses questions often asked by Cisco Unity Administrators is also available.

To Display Online Documentation

Step 1 Click the **Online Documentation** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays the relevant page from the *System Administration Guide for Cisco Unity* in a separate window.

Step 2 To browse to additional topics, click a link included in the displayed topic or listed in the Contents.

To Display Field Help

Step 1 Click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator. Cisco Unity displays a question mark next to each field for which Help is available.

Step 2 For help on a field, click the question mark next to that field.

Step 3 To turn Field Help off, click the **Field Help** icon in the upper right corner of the Cisco Unity Administrator.

To Display the Cisco Unity Administrator FAQ

Step 1 Click the **Cisco Unity Administrator FAQ** link at the bottom of the navigation bar. Cisco Unity displays the FAQ in a separate window.

Or, from the Cisco Unity desktop, click the **Cisco Unity Administrator FAQ** shortcut.

Step 2 Click the available links to browse to questions and answers.

Saving Data

Save newly entered data by clicking the Save icon. Cisco Unity requires you to save new data before moving to another record or to another part of the Cisco Unity Administrator. The following cues remind you when the displayed record contains unsaved data:

- The Save icon is enabled.
- An asterisk is displayed on the title bar next to the record name.
- If you attempt to leave a changed record without saving it, Cisco Unity prompts you to save the record.

Finding Records

A record is the group of settings or collection of data for an individual subscriber, class of service (COS), or other Cisco Unity entity. For example, a subscriber record contains the subscriber account data.

To Find a Subscriber Record

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers page**.

Step 2 Click the **Find** icon.

Step 3 Indicate whether to search by alias, extension, first name, or last name.

Step 4 Enter the applicable alias, extension, or name. You also can enter * to display a list of all subscribers, or enter one or more characters or values followed by * to narrow your search.

Step 5 To search for subscriber accounts that were created on a Cisco Unity server other than your local Cisco Unity server, check the **Search All Cisco Unity Servers** check box.

Step 6 Click **Find**.

Step 7 On the list of matches, click the name of the subscriber to display the record.

To Find Other Types of Records

Step 1 In the Cisco Unity Administrator, go to any page of the applicable record type.

Step 2 Click the **Find** icon.

Step 3 Enter the applicable name. You also can enter ***** to display a list of all records, or enter one or more characters followed by * to narrow your search.

Step 4 Click **Find**.

Step 5 On the displayed list, double-click the applicable record.

Adding Records

Always enter information for a new record in an Add window.

Caution Entering new record information on an existing page will change the displayed record rather than create a new record.

Use the following procedure to add a record, such as a new class of service (COS), distribution list, or call handler. To add a new subscriber, see the "Managing Subscriber Accounts" chapter.

To Add a Record

Step 1 Click the **Add** icon from any COS, distribution list, or call handler page.

Step 2 In the window that is displayed, enter basic identifying information, such as the name of the record.

Step 3 Indicate whether this record is new or based on an existing one. If based on an existing record, click the name of that record on the list.

Step 4 Click **Add**.

CHAPTER 2

Managing Cisco Unity Administrator Accounts

See the following sections in this chapter:

About the Accounts That Can Be Used to Administer Cisco Unity

To access the Cisco Unity Administrator, administrators can use one of the following accounts:

Administration account	This is the account that was selected during installation to administer Cisco Unity. The administration account is automatically associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator
The Active Directory account associated with a Cisco Unity subscriber account that has COS rights to access the Cisco Unity Administrator	In order for administrators to log on to the Cisco Unity Administrator on the Cisco Unity server, this account must be a member of one of the following Admins groups, as applicable: • Domain Admins group (when the Cisco Unity server is a domain controller) • Local Administrators group (when the Cisco Unity server is a member server) Otherwise, the account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server

Until you create a Cisco Unity subscriber account specifically for the purpose of administering Cisco Unity, you must use the Active Directory credentials associated with the administration account that was selected when Cisco Unity was installed to log on to the Cisco Unity Administrator.

Consider using an alternative to the administration account, if you want to do the following:

- Limit the use of the administration account. The COS assigned to the administration account has full system access rights to the Cisco Unity Administrator. This means that not only can the administration account access all pages in the Cisco Unity Administrator, but it also has read, edit, add, and delete privileges for all Cisco Unity Administrator pages.

- Ensure that there are additional accounts available that can be used to access the Cisco Unity Administrator if the administration account is deleted or corrupted.

The Cisco Unity subscriber accounts that are used to access the Cisco Unity Administrator must have the appropriate COS rights. COS rights specify which tasks, if any, administrators can do in the Cisco Unity Administrator. For example, some subscriber accounts that are used for administrator access can be associated with a COS that provides read-only access, or that restricts administrators to access of specific pages in the Cisco Unity Administrator for the purpose of unlocking accounts or changing passwords.

In addition to COS rights, subscriber accounts that are used to access the Cisco Unity Administrator must be associated with an Active Directory account that is enabled.

To create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, complete the procedures in the "Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator" section on page 2-2. If you prefer not to create a specific subscriber account for each administrator who needs to access the Cisco Unity Administrator, you can use the GrantUnityAccess utility to associate one or more Active Directory accounts with a single subscriber account. For more information about using the GrantUnityAccess utility, see the "Granting Administrative Rights to Other Cisco Unity Servers" section on page 2-3.

Note As a best practice, we recommend that Cisco Unity Administrators not use the same subscriber account to log on to the Cisco Unity Administrator that they use to log on to the Cisco PCA to manage their own Cisco Unity accounts. In addition, they should not use Unity service accounts to administer Cisco Unity.

Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator

To create additional subscriber accounts for the purposes of accessing the Cisco Unity Administrator, you use the same procedures that you use for creating regular subscriber accounts (as detailed in the "Managing Subscriber Accounts" chapter. However, if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you will also need to add their Active Directory accounts either to the local Administrators group—when the Cisco Unity server is a member server—or to the Domain Admins group—when the Cisco Unity server is a domain controller. You can do the applicable procedures in this section either before or after you create subscriber accounts. Until this is done, administrators can access the Cisco Unity Administrator only from another computer.

To Add the Active Directory Account to the Local Administrators Group (When the Cisco Unity Server Is a Member Server)

Step 1 On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Computer Management**.

Step 2 In the left pane of the Computer Management MMC, expand **System Tools > Local Users and Groups**.

Step 3 In the left pane, click **Users**.

Step 4 In the right pane, double-click the administration account.

Step 5 In the Properties dialog box, click the **Member Of** tab.

Step 6 Click **Add**.

Step 7 In the Select Groups dialog box, in the top list, double-click **Administrators**.

Step 8 Click **OK** to close the Select Groups dialog box.

Step 9 Click **OK** to close the Properties dialog box.

Step 10 Close the **Computer Management MMC**.

To Add the Active Directory Account to the Domain Admins Group (When the Cisco Unity Server Is a Domain Controller)

Step 1 On the Cisco Unity server, log on to Windows by using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers** or click **Programs > Administrative Tools > Active Directory Users and Computers**.

Step 3 In the left pane, expand the domain, and click **Users**.

Step 4 In the right pane, double-click the name of the administration account.

Step 5 Click the **Members Of** tab.

Step 6 Click **Add**.

Step 7 In the Select Groups dialog box, in the top list, double-click **Domain Admins**.

Step 8 Click **OK** to close the Select Groups dialog box.

Step 9 Click **OK** to close the Properties dialog box.

Step 10 Close **Active Directory Users and Computers**.

Granting Administrative Rights to Other Cisco Unity Servers

Rather than create subscriber accounts on each server for each person who needs to administer Cisco Unity, you can use the GrantUnityAccess utility to associate any number of Active Directory accounts with a single Cisco Unity subscriber account. GrantUnityAccess maintains a table of the associated Active Directory accounts and Cisco Unity subscriber accounts that Cisco Unity references when someone tries to access the Cisco Unity Administrator (regardless of the authentication method used by the Cisco Unity Administrator). This table is used to determine whether to permit someone access to the Cisco Unity Administrator.

Before you use GrantUnityAccess, consider the following:

- The Active Directory account(s) that you want to associate with a subscriber account must either be in the same domain as the Cisco Unity server or in a trusted domain. In addition, if you want administrators to be able to log on to the Cisco Unity Administrator on the Cisco Unity server, you must add the Active Directory account to the applicable Admins group (see the "Creating Subscriber Accounts That Can Be Used to Access the Cisco Unity Administrator" section on page 2-2 for a detailed procedure.) Otherwise, the account must at least have the right to log on locally so that administrators can log on to the Cisco Unity Administrator from a computer other than the Cisco Unity server.
- As a best practice, the Active Directory accounts that are associated with subscriber accounts should require strong passwords. Set your domain account policy in Active Directory to require them.
- You can associate multiple accounts with a single subscriber account.

- You can associate Active Directory account(s) with any subscriber account, as long as the subscriber account has COS rights to access the Cisco Unity Administrator. This includes the administration account that was selected when Cisco Unity was installed.
- Because the administration account is associated with a COS that offers unlimited access to the Cisco Unity Administrator, consider associating the Active Directory account(s) used by administrators with a different subscriber account that you create on each Cisco Unity server—one that has more limited COS rights. In this way, you can customize the level of access for the administrators in your organization.
- If there are several servers that the administrators need access to, you can create a batch file that contains the commands to grant access to the applicable servers. In this way, you can avoid entering the commands repeatedly.

Use the following procedure to run GrantUnityAccess. Note that you cannot run GrantUnityAccess remotely across a network, so you will need to run it on each Cisco Unity server that you want to make accessible, and for each account that you want to map. See the "Sample GrantUnityAccess Arguments" section on page 2-4 for an example of how this utility is used, and for argument syntax details.

To Use the GrantUnityAccess Utility

Step 1 Log on to Windows on the Cisco Unity server by using either the administration account that was selected when Cisco Unity was installed or an Active Directory account that is a member of the local Administrators group on the Cisco Unity server.

Step 2 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 3 In the left pane, expand **Diagnostic Tools**, and double-click **Grant Unity Access** to display a command prompt window.

Step 4 To associate an Active Directory account with a Cisco Unity subscriber account, enter:

GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias>

Sample GrantUnityAccess Arguments

For example, assume that JSmith and KChen are the aliases of administrators who need access to the Cisco Unity Administrator on another Cisco Unity server, and that their Active Directory accounts are in a domain called NewYorkDomain. To associate their Active Directory accounts with the administration account that was selected when Cisco Unity was installed, run GrantUnityAccess two times as follows:

GrantUnityAccess -u NewYorkDomain\JSmith -s <UnitySubscriberAlias for administration account>

GrantUnityAccess -u NewYorkDomain\KChen -s <UnitySubscriberAlias for administration account>

Rather than specifying the administration account, you could associate the Active Directory account for Neil Jones with the subscriber account for Kelly Bader instead:

GrantUnityAccess -u NewYorkDomain\NJones -s KBader

To obtain a list of accounts that have been associated with Cisco Unity subscriber accounts, enter:

GrantUnityAccess -l

To delete an association made previously using GrantUnityAccess, enter:

GrantUnityAccess -u <Domain>\<UserAlias> -s <UnitySubscriberAlias> -d

To display information about these and other arguments, enter:

GrantUnityAccess -?

CHAPTER 3

Call Management Overview

See the following sections in this chapter:

Call Management Tools

Cisco Unity provides the following tools for managing incoming and outgoing calls:

Call Handlers

Call handlers answer calls and can take messages; provide menus of options (for example, “For customer service press 1, for sales press 2...”); route calls to subscribers and to other call handlers; and play audiotext (prerecorded information). See the “Call Handler Settings Overview” section on page 4-1 for more information.

Directory Handler

Directory handlers provide directory assistance by playing an audio list that subscribers and unidentified callers use to reach subscribers and to leave messages. See the “Directory Handler Settings Overview” section on page 5-1 for more information.

Interview Handlers

Interview handlers collect information from callers by playing a series of questions and then recording the answers. See the “Interview Handler Settings Overview” section on page 6-1 for more information.

Call Routing Tables

Call routing tables allow you to define how calls are initially routed, based on criteria such as the phone number of the caller and the schedule. When you have set up call handlers, interview handlers, and the directory handler, as well as extensions for subscribers, you can route calls to the applicable person or handler by modifying the call routing tables. See the "Call Routing Tables Overview" section on page 3-3 for more information.

Restriction Tables

Restriction tables control outgoing calls by allowing you to specify the numbers that Cisco Unity can dial for transferring calls, for notifying subscribers of messages, and for delivering faxes. See the "Restriction Tables Overview" section on page 7-1 for information on how to set up and use restriction tables.

Creating and Implementing a Call Management Plan

Careful planning for your system components—call handlers, interview handlers, directory handlers, and call routing tables—is key to setting them up efficiently. Creating a call management map is a way to document your plan.

When you have considered how your call management plan ought to work, you can create a sketch that shows specifically how the handlers connect to one another. Include a menu of one-key dialing options and all possible navigation choices (such as reaching a call handler by dialing an extension or via a routing rule). You can also include the predefined Cisco Unity call handlers in your plan.

After you have mapped your plan, write detailed scripts for the greeting of each call handler to use during the recording session.

When you are ready to set up your system of call handlers, start from the bottom up. First create the call handlers to which calls are routed. You will select these "destination" call handlers when you create the call handlers that route calls to them. You also need to create Cisco Unity accounts for the subscribers to which call handlers will transfer before creating those call handlers.

In addition to mapping call handlers, you also need to plan call routing tables. Another alternative is to assign extensions to some of your call handlers and to route incoming calls to those extensions by using a call routing table.

Routing Callers by Using One-Key Dialing

With one-key dialing, you can offer callers a menu of choices. One-key dialing enables you to designate a single digit to represent a subscriber extension, call handler, interview handler, or directory handler. Instead of entering the full extension, the caller presses a single key.

Callers can bypass one-key dialing. You set the system to pause a certain number of seconds for additional key presses before routing the call according to the way you have set up a one-key dialing menu. These pauses allow callers to press full extension IDs to bypass one-key dialing menus, even during the handler greeting.

You can also lock certain keys to take the caller directly to the action programmed for that key without waiting for an additional key press.

Use the handler greeting to tell callers about the one-key options they have, and whether they are allowed to enter an extension during the greeting.

Call Routing Tables Overview

Call routing tables are used to route incoming calls to the operator or to specific subscribers, call handlers, directory handlers, or interview handlers. In addition, call routing tables are used to route subscribers to the subscriber logon conversation.

Cisco Unity has two call routing tables—one for direct calls and one for forwarded calls—that handle calls from subscribers and from unidentified callers. Each table contains predefined routing rules, and you can create additional rules to route calls as needed. Set up your directory handlers, call handlers, and interview handlers first, and then modify or create call routing rules for each table as needed to route incoming calls correctly.

Direct Calls Call Routing Table

The Direct Calls call routing table handles calls from subscribers and unidentified callers that are dialed directly to Cisco Unity. The predefined routing rules for the Direct Calls call routing table are:

- Attempt Sign-In—Calls from subscribers are routed to the subscriber logon conversation.
- Default Call Handler—Calls from unidentified callers are routed to the Opening Greeting.

Forwarded Calls Call Routing Table

The Forwarded Calls call routing table handles calls that are forwarded to Cisco Unity from either a subscriber extension or from an extension that is not associated with a subscriber account (such as a conference room). The predefined routing rules for the Forwarded Calls call routing table are:

- Attempt Forward to Greeting—All calls forwarded from a subscriber extension are routed to the subscriber greeting.
- Default Call Handler—Calls forwarded from an extension that is not associated with a subscriber account are routed to the Opening Greeting.

You can change the order of the Attempt Sign-In and Attempt Forward to Greeting rules in the respective routing tables, but the Default Call Handler rule is always the last entry for both tables. You cannot modify or delete the predefined rules.

How Call Routing Rules Work

Call routing tables consist of a series of rules that let you route incoming calls based on the information that Cisco Unity may have about a call, such as the calling phone number (ANI or caller ID), the trunk or port on which the call comes in, the dialed phone number (DNIS), the forwarding station, and the schedule.

When Cisco Unity receives a call, it first determines if it is a direct or forwarded call based on the information contained in the serial or DTMF packet sent by the phone system, and then applies the applicable call routing table. If the call information matches all of the settings for the first rule, the call is routed as specified in the rule. If any call information does not match the settings specified in the first rule, the call information is then compared to the settings of the second rule, and so on, until a rule is found that matches all the characteristics of the call.

The integration between the phone system and Cisco Unity determines the information that is provided about a call (for example, call type, port, trunk, calling number, and dialed number). The schedule is determined by the date and time the call is received.

To set up routing rules correctly, you need to know what information your integration provides. See the Call Information section in the Cisco Unity integration guide for your phone system for this information (Cisco Unity integration guides are available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html). You can also use the Cisco Unity Call Viewer to see the types of call information that your integration provides to Cisco Unity for inbound calls. To access the Call Viewer, on the Cisco Unity server desktop, double-click the Cisco Unity Tools Depot icon. In the left pane of the Tools Depot window, in the Switch Integration Tools directory, double-click Call Viewer.

The following examples show how call routing tables are used in Cisco Unity to route calls.

Example 1

In Table 3-1, calls that meet the criteria specified in the Operator rule settings—any direct external call received while the Weekdays schedule is active—are transferred to the operator. Calls that do not meet this criteria are routed as specified by one of the other call routing rules in the table. In this case, any direct external calls received on the weekends will be routed to the Opening Greeting, according to the Default Call Handler rule.

Table 3-1 Direct Calls Call Routing Table

Rule	Status	Call Type	Port	Trunk	Dialed Number	Calling Number	Schedule	Sent Call To	Language
Operator	On	External calls	Any	Any	Any	Any	Weekdays	Attempt transfer for operator	Inherited
Attempt Sign-in	On	Both	Any	Any	Any	Any	Always	Attempt Sign-in	English
Default Call Handler	On	Both	Any	Any	Any	Any	Always	Attempt transfer for Opening Greeting	Inherited

Example 2

In Table 3-2, calls forwarded from specific extensions—1234 and 5678—are routed according to the Product Info and Customer Service rules, respectively. Calls that do not match the extension (or forwarding station) in either of the first two rules are routed according to the two remaining rules.

Table 3-2 Forwarded Calls Call Routing Table

Rule	Status	Call Type	Forwarding Station	Dialed Number	Calling Number	Schedule	Sent Call To	Language
Customer Service	On	Both	5678	Any	Any	Always	Attempt transfer for Customer Service	Inherited
Product Info	On	Both	1234	Any	Any	Always	Send to greeting for Product Info	English
Attempt Forward	On	Both	Any	Any	Any	Always	Attempt Forward	English
Default Call Handler	On	Both	Any	Any	Any	Always	Attempt transfer for Opening Greeting	Inherited

Creating and Modifying Call Routing Rules

Although you cannot modify the predefined routing rules in the Direct Calls and Forwarded Calls call routing tables, you can create additional call routing rules for each call routing table and modify them as needed.

To Create a Call Routing Rule

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- For direct calls, go to the **Call Management > Call Routing > Direct Calls** page.
- For forwarded calls, go to the **Call Management > Call Routing > Forwarded Calls** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Call Routing Rule dialog box, enter the name of the new rule in the Name field.

Step 4 Click the **Add** button.

Step 5 Specify the settings for the new call routing rule, as applicable, and then click the **Save** icon.

Note When you create a new rule, you need to specify only the criteria that will be used to route the call, and can leave the other fields on the page blank. A blank field matches everything. For example, if you leave the Ports field blank, the rule applies to calls from all ports.

To Modify a Call Routing Rule

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- For direct calls, go to the **Call Management > Call Routing > Direct Calls** page.
- For forwarded calls, go to the **Call Management > Call Routing > Forwarded Calls** page.

Step 2 In the routing table, click the rule that you want to modify.

Step 3 Change settings as applicable in the fields above the table, and then click the **Save** icon.

Creating and Modifying Schedules

Schedules are one of the variables that Cisco Unity uses to manage calls. The standard and closed subscriber and call handler greetings play according to the days and times that you specify in a schedule.

Cisco Unity offers two predefined schedules: All Hours – All Days, and Weekdays, both of which can be modified. In addition, you can create up to 64 schedules for your organization to accommodate the standard working hours of different groups of employees. You can use either of the predefined schedules, or a new schedule that you create, as the default schedule for Cisco Unity. The default schedule is used for all call handlers, subscriber templates, and call routing tables, unless you specify a different schedule for each call handler, subscriber account, or call routing table to follow.

For each schedule that you create or modify, you identify the hours and days that make up the standard and closed hours, and whether the schedule changes for holidays:

Standard hours	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.)
Closed hours	The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.
Holidays	The time range defined on the System > Holidays page when the organization is closed. See the "Identifying Days as Holidays" section on page 3-7 for information about identifying holidays.

To Create a New Schedule

Step 1 In the Cisco Unity Administrator, go to the **System > Schedules** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Schedule dialog box, enter information as applicable in the Name field.

Step 4 Select **New Schedule** or **Based on Existing Schedule**. If you select Based on Existing Schedule, select the applicable schedule in the Based On field.

Step 5 Click the **Add** button.

Step 6 Check the **Observe Holidays** check box, if applicable.

Step 7 Click boxes on the schedule grid until all open (standard) half hours are white and all closed half hours are gray. Note that you can use the **Copy Day's Schedule** field and **>>** functions to avoid clicking the same blocks for more than one day.

Step 8 Click the **Save** icon.

Step 9 To use this new schedule as the Cisco Unity default schedule, do the following "To Specify the Default Schedule" procedure.

To Specify the Default Schedule

Step 1 In the Cisco Unity Administrator, go to the **System > Schedules** page, and click **Change Default Schedule** from any schedule page.

Note When you click the link, you leave the schedule page, and move to the System > Configuration > Settings page.

Step 2 In the Default Schedule field, click the schedule you want to use as the default for new call handlers, subscriber templates, and call routing tables.

Step 3 Check the **Use 24-Hour Time Format for Conversation and Schedules** check box to use a 24-hour time format for all schedules, if applicable.

Step 4 Click the **Save** icon.

To Modify an Existing Schedule

Step 1 In the Cisco Unity Administrator, go to the **System > Schedules** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the schedule that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

Step 5 To use this new schedule as the system default schedule, do the "To Specify the Default Schedule" procedure on page 3-6.

Identifying Days as Holidays

When a Holiday setting is in effect, Cisco Unity plays closed greetings and observes closed transfer rules. You can set up several years of holidays at a time, and you can copy the holidays from one year to the next, adjusting dates as necessary. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

To Identify Days as Holidays

Step 1 In the Cisco Unity Administrator, go to the **System > Holidays** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Holiday dialog box, select the month, day, and year of the holiday.

Step 4 Click the **Add** button.

To Modify a Holiday

Step 1 In the Cisco Unity Administrator, go to the **System > Holidays** page.

Step 2 Click the date of the holiday listed for the applicable year.

Step 3 In the Edit Holiday For field, change settings as applicable, and then click the **Save** icon.

CHAPTER 4

Managing Call Handlers

See the following sections in this chapter:

Call Handler Settings Overview

Call handlers answer calls, greet callers with recorded prompts and provide them with information and options, route calls, and take messages. They are a basic component of Cisco Unity. Your plan for call handlers can be simple, using only the predefined Cisco Unity call handlers, or you can create an unlimited number of new call handlers. You may want to use call handlers in the following ways:

- As an automated attendant—A call handler can be used in place of a human operator to answer and direct calls by playing greetings and responding to touchtones. The automated attendant can provide a menu of options (for example, “For Sales, press 1; for Service, press 2; for our business hours, press 3.”).
- To offer prerecorded audiotext—A call handler can be used to provide information that customers request frequently (for example, “Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.”).
- As a message recipient—A call handler can be used to take messages for the organization (for example, “All of our customer service representatives are busy. Please state your name, phone number, and account number, and we will return your call as soon as possible.”).
- To transfer calls—A call handler can be used to route callers to a subscriber (for example, after hours, you could transfer calls that come to a technical support call handler directly to the cell phone of the person who is on call), or to another call handler.

Predefined Call Handlers

Cisco Unity comes with the following predefined call handlers, which you can modify but not delete. Note that you will at least want to modify the greetings for these call handlers.

Opening Greeting	Acts as an automated attendant, playing the greeting that callers first hear when they call your organization, and performing the actions you specify. The Default Call Handler Call Routing rule transfers all incoming calls to the Opening Greeting call handler. By default, the Opening Greeting call handler allows callers to press * to reach the Sign-in conversation, or press # to reach the Operator call handler. Messages left in the Opening Greeting call handler are sent to the Example Administrator.
Operator	Calls are routed to this call handler when callers press "0" or do not press any key, (the default setting) as stated in the Cisco Unity conversation. You can set up the Operator call handler so that callers can leave a message or be transferred to a live operator. By default, the Operator call handler allows callers to press * to reach the Sign-in conversation, or press # to reach the Opening Greeting call handler. Messages left in the Operator call handler are sent to the Unaddressed Messages distribution list.
Goodbye	Plays a brief goodbye message and then hangs up if there is no caller input. By default, the Goodbye call handler allows callers to press * to reach the Sign-in conversation, or press # to reach the Opening Greeting call handler. If you change the After Greeting action from Hang Up to Take Message, then messages left in the Goodbye call handler are sent to the Example Administrator.

Creating and Modifying Call Handlers

You can use the procedures in this section to create new call handlers or to modify existing ones by using the Cisco Unity Administrator. You can also use the Bulk Edit utility to make changes to multiple call handlers at once. 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.)

Timesaver

Depending on the hardware that your Cisco Unity server uses, if you have 1,000 or more call handlers, we do not recommend that you use the Cisco Unity Administrator to create additional call handlers or to modify existing call handlers, as the process can be lengthy. Instead, we recommend that you use the Audio Text Manager to create additional call handlers, and use either the Bulk Edit utility or Audio Text Manager to modify them.

To manage call handler greetings when you or the call handler owner(s) that you assign cannot access the Cisco Unity Administrator, you can use the Cisco Unity Greetings Administrator. For more information, see the "Cisco Unity Greetings Administrator Overview" section on page 26-1 and the "Using the Cisco Unity Greetings Administrator to Manage Call Handler Greetings" section on page 26-3.

To Create a New Call Handler in the Cisco Unity Administrator

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Call Handlers** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Call Handler dialog box, enter information as applicable in the Name field.

Step 4 Select **New Handler** or **Based on Existing Handler**. If you select Based on Existing Handler, select the applicable call handler in the Based On field.

Note that if you based your new call handler on an existing one, you reuse all of the settings, including recorded greetings. For this reason, make sure to rerecord the greeting for the new call handler.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new call handler, and then click the **Save** icon.

To Modify a Call Handler in the Cisco Unity Administrator

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Call Handlers** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the call handler that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

About Call Handler Transfer Settings

Call transfer settings specify how Cisco Unity transfers calls 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.)

When transferring a call to a subscriber extension, 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 call screening and call holding options on indirect calls:

- 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.
- 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, and therefore the total number of callers that can be holding in the queue at any one time is limited by the number of available ports.

  The default wait time in the call holding queue for the first caller in the queue is 25 seconds. If the caller is still on hold after this amount of time, Cisco Unity asks whether the caller wants to continue holding, to leave a message, or to try another extension. If the caller does not press 1 to continue holding, press 2 to leave a message, or dial another extension, 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. (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 for more information on call holding.)

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

Each call handler can 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.

About Call Handler Greetings Settings

Each subscriber and call handler can have up to five greetings. The greeting settings specify which greetings are enabled, the greeting source, and the actions that Cisco Unity takes during and after each greeting.

Note that Cisco Unity plays the greetings that you enable for the applicable situation, while 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.

Call handler owners can select a different call handler greeting or record the call handler greetings from the Call Management > Call Handlers > Greetings page in the Cisco Unity Administrator, or they can use the Cisco Unity Greetings Administrator to do so over the phone. For more information, see the “Cisco Unity Greetings Administrator Overview” section on page 26-1.

CHAPTER 5

Managing Directory Handlers

See the following sections in this chapter:

Directory Handler Settings Overview

Directory handlers provide directory assistance in Cisco Unity that callers can use to reach subscribers. When a caller searches on a subscriber name or part of a name, a directory handler looks up the extension and routes the call to the correct subscriber. Note that subscribers cannot be accessed by using directory handlers unless they have recorded names.

Each directory handler contains settings that specify how it searches for names, what it does when it finds one or more matches, and what it does when it detects no caller input.

The multiple directory handler feature provides quick, effective, and secure directory searches for systems with hundreds or thousands of subscribers. Multiple directory handlers are also used for call routing in headquarters and branch office deployments where Cisco Unity provides centralized call processing. Administrators can create as many directory handlers as they need to manage caller searches for subscribers.

Creating and Modifying Directory Handlers

You can use the default pre-defined directory handler or any other existing directory handler as a template to create additional directory handlers. Create as many directory handlers as needed to route calls to subscribers by using available filters such as location, class of service, and public distribution list membership.

You can also modify or delete directory handlers; however, note that the default directory handler can be modified, but not deleted.

Subscribers can be listed in more than one directory handler.

Because directory handlers do not have greetings, use call handlers or one-key dialing to route callers to a directory handler, and use the call handler greeting to explain caller options for each directory handler.

To Create a Directory Handler

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Directory Handlers** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Directory Handler dialog box, enter information as applicable in the Name field.

Step 4 Select **New Handler** or **Based on Existing Handler**. If you select Based on Existing Handler, select the applicable directory handler in the Based On field.

If you base a new directory handler on an existing one, all of the settings are copied except for the extension and recorded name. If you select New Handler, the new directory handler is based on the default directory handler.

Step 5 Click the **Add** button.

Step 6 Specify the settings for your new directory handler, as applicable, and then click the **Save** icon.

Note that there may be a delay in synchronizing and accessing new directory handlers. See the "Synchronizing Directory Handlers with the Subscriber Database" section on page 5-3 for more information.

To Modify a Directory Handler

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Directory Handler** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the directory handler that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

Note that there may be a delay in synchronizing and accessing new directory handlers. See the "Synchronizing Directory Handlers with the Subscriber Database" section on page 5-3 for more information.

To Delete a Directory Handler

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Directory Handler** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the directory handler that you want to delete.

Step 4 Click the **Delete** icon.

Step 5 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 6 In the left pane, under Diagnostic Tools, double-click **DbWalker**.

Step 7 In the Automatic Repairs tab, check the following check boxes, as applicable, to initiate repairs:

- **Remove Orphaned Call Handlers**
- **Delete Empty Private Distribution Lists**
- **Set Broken User Keys to Ignore**
- **Remove References to Missing Greeting or Voice Name WAV Files**

Tip Alternatively, you can run the Cisco Unity Directory Walker (DbWalker) utility without any check boxes checked to determine whether there are links to the deleted directory handler from other objects, such as call handlers, as well as to identify other database problems. Based on what you learn from the DbWalker output, you can then run the utility a second time, with your choice of automatic repairs selected.

Step 8 In the Logging pane, enter the location for the output log file.

Step 9 Click **Walk Database**.

Step 10 Click **OK**, then click **OK** again to view the output log to see the errors that were identified and what automatic repairs, if any, were made.

Step 11 Click **Exit**.

Synchronizing Directory Handlers with the Subscriber Database

Depending on the complexity of the Cisco Unity system configuration, synchronization of a new directory handler can take several minutes to several hours to complete. Factors that can affect synchronization speed include:

- System configuration, including multi-domain environments, organization unit structure, synchronization timer setting, and public distribution list complexity
- Cisco Unity Digital Networking configuration
- Number of subscribers and public distribution lists

When a directory handler is scoped by a distribution list, the membership is synchronized from Active Directory into the Cisco Unity SQL Server database. Changing the distribution list by which the directory handler is scoped requires a synchronization. This synchronization takes place when the Cisco Unity directory services (AvDSAD and AvDSGlobalCatalog) poll the directory for any changes to be applied to the SQL Server database, which usually occurs within 15 to 20 minutes after the directory handler scope change is made in the Cisco Unity Administrator.

If an outside caller calls into Cisco Unity and navigates to a recently created or modified directory handler on which synchronization has not yet completed, the Cisco Unity conversation may not present the full list of the directory members and/or may fail to find some directory members. This can also occur if the system administrator calls into Cisco Unity to verify directory handler additions or changes immediately after the changes are made in the Cisco Unity Administrator.

To initiate an immediate synchronization, do the following procedure.

To Manually Synchronize the Cisco Unity Database and Verify That Subscribers Can Be Located in the Directory Handler

Step 1 In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page.

Step 2 In the Replicate Cisco Unity Directory Objects section, click **Changed Objects**.

The Settings page is refreshed and the database changes will be synchronized in the background.

Step 3 Wait a few minutes, then call in to Cisco Unity and confirm that the subscriber(s) can be located in the directory handler.

Step 4 If the subscriber(s) still cannot be located, confirm that they have recorded names. Subscribers cannot be accessed by using directory handlers unless they have recorded names.

Limiting Directory Handler Searches

The search options settings specify whether a directory handler searches for subscribers by using first name first, or last name first. Additionally, these settings allow you to restrict directory handler searches to the local Cisco Unity server, a public distribution list, a class of service, or if your organization uses Digital Networking to network Cisco Unity servers within a dialing domain, to expand searches to Cisco Unity servers at other locations.

Note For more information about dialing domains, see the "Dialing Domains" section in the "Digital Networking" chapter of the *Networking Guide for Cisco Unity*. (The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.)

Even if you have Digital Networking set up, you may want to consider limiting directory handler searches to the local server if either of the following conditions is true:

- If there are a large number of subscribers with the same name in your organization. In this situation, if you enable directory handler searches for multiple locations, the list of matching names presented to callers may be too long to be useful.
- If it is important to retain the individual call transfer settings for subscribers associated with other networked locations. If you enable directory handler searches for multiple locations, any calls transferred from a directory handler to subscribers not associated with the local server are automatically handled by the phone system—rather than by Cisco Unity—even if these subscribers are set up for supervised transfers on their own local Cisco Unity servers. As a result, the call screening, call holding, and announce features would not be available on these calls.

CHAPTER 6

Managing Interview Handlers

See the following sections in this chapter:

Interview Handler Settings Overview

Interview handlers collect information from callers by playing a series of questions that you have recorded, and then recording the answers offered by callers. For example, you might use an interview handler to take sales orders or to gather information for a product support line.

When a call is routed to an interview handler, the interview handler plays the first recorded question, then plays a beep, then records the answer. Cisco Unity stops recording either when the response reaches the maximum recording time that you have specified, or when the caller stops speaking. Cisco Unity then plays the second question, and so on. When all the answers have been recorded, they are forwarded as a single voice message, with beeps separating the answers, to the recipient that you designate.

By default, this recipient is the Example Administrator. If you want these messages to be routed to another recipient, choose a subscriber (such as the operator) or a distribution list as the recipient. Do not delete the Example Administrator account unless you have assigned the applicable subscribers or public distribution lists to review the messages sent to the Interview call handler.

About the Example Interview Handler

Cisco Unity comes with a predefined interview handler called Example Interview, which you can modify but not delete. You can have callers routed to this interview handler when they do not press any phone keys during the Opening Greeting, or by selecting it as the after-greeting action on the Greetings page of the call handler that plays the Opening Greeting.

The Example Interview handler asks the following questions:

- What person or department are you trying to reach?
- What is your name?
- What is your phone number?
- What are the best times to reach you?
- Is there any other information you would like to leave?

Creating and Modifying Interview Handlers

You can modify the Example Interview handler, and you can create new ones.

To Create a New Interview Handler

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Interview Handler** page.

Step 2 Click the **Add** icon.

Step 3 In the Add an Interview Handler dialog box, enter information as applicable in the Name field.

Step 4 Select **New Interview Handler** or **Based on Existing Interview Handler**. If you select Based on Existing Interview Handler, select the applicable interview handler in the Based On field.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new interview handler, and then click the **Save** icon.

To Modify an Interview Handler

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Interview Handler** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the interview handler that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

CHAPTER 7

Managing Restriction Tables

See the following sections in this chapter:

Restriction Tables Overview

Restriction tables allow you to control the phone numbers that subscribers and administrators can use for:

- Transferring calls—including both the numbers subscribers can enter for transferring their calls, and the numbers that unidentified callers can enter when using Caller system transfers. (For more information on Caller system transfers, see the "Setting Up System Transfers" section on page 15-11.)
- Recording and playback by phone from Cisco Unity applications, when the phone is the designated recording and playback device in the Media Master. (The Media Master is available in the Cisco Unity Administrator, the Cisco Unity Assistant, the Cisco Unity Inbox, and ViewMail.)
- Delivering faxes to a fax machine.
- Sending message notifications.
- Sending AMIS messages.

For example, you can specify that subscribers have calls transferred only to internal extensions or that faxes are delivered only to local phone numbers. Restriction tables are applied regardless of how a subscriber or administrator accesses Cisco Unity. They do not affect the phone numbers that subscribers and administrators can dial when they are not logged on to Cisco Unity.

Each class of service specifies for its members a restriction table for call transfers, one for message notification, and one for fax deliveries. The restriction table can be the same for all three, or different for each. Note, however, that the AMIS restriction table is not associated with a class of service; there is only one system-wide Restriction Table that controls AMIS message delivery.

Predefined Restriction Tables

Cisco Unity 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.

{Default Outdial}	Restricts numbers for message notifications. Also restricts the subscriber extensions that Cisco Unity dials when the phone is selected as the recording and playback device in the Media Master. (The Media Master is available in the Cisco Unity Administrator, the Cisco Unity Assistant, the Cisco Unity Inbox, and ViewMail.)
{Default Transfer}	Restricts numbers for call transfers.
{Default Fax}	Restricts numbers for fax delivery.
{Default AMIS}	Determines which AMIS delivery numbers can be processed immediately and which delivery numbers must wait for the AMIS schedule to become active.
CS_Default_System_Transfer	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 Cisco Unity subscriber. By default, the table does not allow Cisco Unity to dial any numbers.

How Restriction Tables Work

When a subscriber uses the Cisco Unity Assistant or the Cisco Unity conversation to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer, or when subscribers use Caller system transfers to transfer to a number that they specify, Cisco Unity applies the applicable restriction table to verify that the phone number entered is allowed. The same thing happens when an administrator uses the Cisco Unity Administrator to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer. In each case, the restriction table used is the one associated with the subscriber or administrator who is changing the number.

For example, if a subscriber uses the Cisco Unity Assistant to enter a phone number to set up a message notification device, Cisco Unity applies the restriction table associated with class of service of that subscriber, and displays an error message if the phone number is not allowed. But when an administrator changes a message notification number for a subscriber by using the Cisco Unity Administrator, Cisco Unity applies the restriction table associated with the administrator class of service, not the class of service of the subscriber. Therefore, an administrator can, when necessary, override the limitations of the class of service of a particular subscriber.

Each row of a restriction table is made up of a dial string. Each dial string consists of a call pattern and a setting that specifies whether numbers matching the call pattern are permitted for use. The restriction table is applied when a subscriber or an administrator attempts to change a number controlled by a restriction table, not when Cisco Unity tries to complete a transfer or delivery. (Note, however, that the AMIS restriction table is applied every time a message is sent to an AMIS subscriber or an AMIS location.) To protect Cisco Unity from toll fraud and unauthorized use when subscribers use Caller system transfers, subscribers must log on to Cisco Unity, enter the number that they want to transfer to, and Cisco Unity performs the transfer only when the CS_Default_System_Transfer restriction table permits it.

When a restriction table is applied to a number (such as a pager number for a message notification), Cisco Unity compares the number with the call pattern of the first dial string in the restriction table. If the number does not match the call pattern, Cisco Unity then compares the number with the call pattern in the second dial string, and so on, until it finds a match. When Cisco Unity finds a match, it either permits or restricts the use of this number as specified in the dial string.

Restriction tables are commonly used to permit or restrict the use of the following:

- Specific numbers, such as an extension.
- Numbers that are greater than or less than a specific length.
- Numbers that contain a specific digit or pattern of digits, such as an external access code followed by a long-distance access code.

For example, the restriction table in Table 7-1 restricts most long distance phone numbers, but permits extensions starting with "91." In this case, if a subscriber enters "9123" as a transfer number, Cisco Unity first compares the number to the call pattern in Dial String 0, which restricts all numbers that begin with "91" and are followed by at least seven digits. Because the number entered does not match the call pattern, Cisco Unity then compares the number to Dial String 1, which restricts all numbers that begin with "9011" and are followed by at least seven digits. Finally, Cisco Unity compares the number to the last dial string, which contains the wildcard character that matches all numbers of any length. Because the Allow This String field is set to Yes for this dial string, Cisco Unity permits this number to be used.

Table 7-1 Example 1

Dial String	Call Pattern	Allow This String
0	91???????*	No
1	9011???????*	No
2	*	Yes

The restriction table in Table 7-2 restricts long distance phone numbers and numbers less than four digits long. In this example, "9" is the external access code for the phone system, and "1" is the long-distance access code. Dial String 0 restricts any number beginning with "91," while numbers less than four digits in length are restricted by Dial String 2. Thus, the only numbers permitted by this restriction table have at least four digits, and are not long distance phone numbers.

Table 7-2 Example 2

Dial String	Call Pattern	Allow This String
0	91*	No
1	????*	Yes
2	*	No

Creating and Modifying Restriction Tables

You can modify the predefined restriction tables, and you can create up to 100 new ones. You can also add up to 100 dial strings to a table. New dial strings are automatically inserted into the restriction table as Dial String 0. Note that the order of the dial strings is very important because Cisco Unity sequentially

compares a phone number to the call patterns in the restriction table, starting with Dial String 0. If a number matches more than one call pattern, the number is handled according to the first call pattern it matches.

You can indicate call patterns by entering specific numbers or by using the following special characters as wildcards:

*	Matches zero or more digits.
?	Matches exactly one digit. Use ? as a placeholder for a single digit.
#	Corresponds to the # key on the phone.

By default, all restriction tables have * as the call pattern in the last dial string of the table; you cannot modify this call pattern setting. It prevents a case in which the entered number does not match any call pattern in the table. However, you can change the Allow This String field setting for this dial string to either permit or restrict a number.

To Create a New Restriction Table

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Restriction Tables** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Restriction Table dialog box, enter information as applicable in the Name field.

Step 4 Select **New Restriction Table** or **Based on Existing Restriction Table**. If you select Based on Existing Restriction Table, select the applicable restriction table in the Based On field.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new restriction table, and then click the **Save** icon.

To Modify a Restriction Table

Step 1 In the Cisco Unity Administrator, go to any **Call Management > Restriction Tables** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the restriction table that you want to modify.

Step 4 Do one of the following:

- To add a dial string, click **Add Dial String** and enter settings for the new dial string as applicable.
- To delete a dial string, click the dial string number in the table at the bottom portion of the Restriction Tables page, and then click **Remove Dial String**.
- To modify a dial string, click the dial string number in the table at the bottom portion of the Restriction Tables page, and change settings as applicable.

Step 5 Click the **Save** icon.

CHAPTER 8

Messaging and Default Accounts Overview

Cisco Unity uses default accounts to provide example configurations for a subscriber and for an administrator; to provide an owner for default entities involved in message handling, such as call handlers and distribution lists; and to serve as members of default classes of service.

See the following sections:

About Default Accounts

During the installation of Cisco Unity, the installer is asked to choose the account that will be used to administer Cisco Unity. The purpose of this account is to allow administrator access to the Cisco Unity Administrator for initial setup. (See the "About the Accounts That Can Be Used to Administer Cisco Unity" section on page 2-1 for more information about administrative accounts.)

In addition to the account that is used to access the Cisco Unity Administrator, Cisco Unity creates several other default accounts and public distribution lists that you use when setting up the system. The Cisco Unity default accounts are detailed below.

Example Administrator

During installation, Cisco Unity creates the Example Administrator account based on the {Default Administrator} template. The account is assigned to the Default Administrator class of service, which offers the highest level of system access.

The Example Administrator has an Exchange mailbox and an Active Directory account. The account alias is EAdministrator, and the default extension is 99999. The default phone password for the Example Administrator is 12345. (Note that the default password may be different for your system. If your system is a new installation, the installer was prompted to change the default phone password for the {Default Administrator} template during installation. However, if your system was upgraded from a version earlier than Cisco Unity version 4.0(4), the installer was not prompted to change the default phone password during installation.)

To help protect Cisco Unity from unauthorized access and toll fraud, it is a good idea to specify a long—20 or more digits—and non-trivial password for this account. You can change the phone password for the Example Administrator account on the Subscribers > Subscribers > Phone Password page in the Cisco Unity Administrator at any time.

The Example Administrator account serves as a default owner, message recipient, and member of the following Cisco Unity entities:

- Unaddressed Messages distribution list (by default, the Example Administrator is the only member of this distribution list)
- All Subscribers distribution list
- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler
- Default Directory handler
- Default Administrator Class of Service (by default the Example Administrator is the only account with this class of service)

The Example Administrator subscriber account cannot be deleted from the Cisco Unity Administrator. In fact, the account includes the instructions “Do Not Delete” as part of the subscriber name. However, the account can be deleted if necessary, by using SQL Server and Active Directory tools. For example, you might want to delete the account if the licensed subscriber limit has been reached, or if the account is perceived to be a security hazard even with a strong password.

Do not delete the Example Administrator account unless you have finished assigning the appropriate subscriber(s) or public distribution list(s) as message recipients or members (as applicable) of the Cisco Unity entities with which the account is associated. For more information on the impact of deleting the Example Administrator account, see the “Deleting Subscriber Accounts” section on page 21-29.

Unity Messaging System

The Unity Messaging System account sends notification when a Cisco Unity report is complete. This account also acts as a surrogate sender for messages from unidentified callers. Thus, subscriber messages from unidentified callers are identified as coming from the Unity Messaging System mailbox. This account also receives nondelivery receipts (NDRs) for voice messages that cannot be delivered—for example, when a subscriber mailbox is full—which it then forwards to the public distribution list called Unaddressed Messages.

The alias for this account is Unity_<Servername>. The account cannot be seen in the Cisco Unity Administrator but can be seen in Active Directory Users and Computers. The mailbox has the display name Unity Messaging System.

We recommend that you run the Message Store Manager Utility report on a regular basis to confirm that the Unity_<Servername> mailbox is empty (or you can view the mailbox by using Exchange System Manager). However, do not set a mailbox size limit for the Unity_<Servername> mailbox. The Unity_<Servername> mailbox should not have any messages in it, but setting a mailbox size limit may adversely affect messages passing through this mailbox.

About Message Handling

See the following sections:

How Cisco Unity Handles New Messages

When a subscriber listens to a new message, depending on the action that the subscriber takes while listening, Cisco Unity will either mark the message as read, or will leave the message marked as a new message.

For a new message, the following actions by the subscriber either during or after message playback will mark the message as read:

- Save
- Delete
- Skip message, mark as saved
- Hang-up (Note however that the message is marked as read only if the Mark a Message as Saved Upon Hang-up or Disconnection setting is enabled for the subscriber; otherwise, the message is marked as new)

For a new message, the following actions by the subscriber either during or after message playback will leave the message marked as new:

- Reply (and reply to all)
- Forward
- Skip message, save as new
- Skip message, save as is
- Play message properties
- Toggle urgent flag
- Play previous message
- Play next message
- Play first message
- Play last message
- Find a message by number
- Send quick message
- Call the subscriber (live reply)
- Hang-up (Note however that the message is marked as new only if the Mark a Message as Saved Upon Hang-up or Disconnection setting is disabled for the subscriber; if the setting is enabled, the message is marked as read)

How Cisco Unity Handles Full Mailboxes

This section explains what Cisco Unity subscribers and callers experience when subscribers have full mailboxes.

What Subscribers Experience When Their Mailboxes Exceed Their Limits

Microsoft Exchange dictates the storage limits for subscriber mailboxes. There are three storage limits in Exchange, and the Cisco Unity phone conversation and the Cisco Unity Inbox warn subscribers when they have reached each limit:

- Issue Warning—When subscriber mailboxes reach the specified value for this storage limit, Cisco Unity notifies subscribers when they log on to Cisco Unity by phone by playing the prompt, "Your Inbox is almost full. If your Inbox exceeds its storage limit, you will not be able to send or receive new messages. To reduce the size of your Inbox, delete some messages now. You will be reminded to do so each time you log on until your Inbox is no longer close to its storage limit." A similar message is displayed in the Cisco Unity Inbox.
- Prohibit Send—When subscriber mailboxes reach the specified value for this storage limit, subscribers are prohibited from sending messages. Cisco Unity notifies subscribers when they log on to Cisco Unity by phone and when they attempt to send a message by playing the prompt, "Your Inbox is full. You cannot send new messages. Delete some messages now." A similar message is displayed in the Cisco Unity Inbox.
- Prohibit Send and Receive—When subscriber mailboxes reach the specified value for this storage limit, subscribers are prohibited from sending and receiving messages. Cisco Unity notifies subscribers when they log on to Cisco Unity by phone and when they attempt to send a message, by playing the prompt, "Sorry. Your Inbox is full. You cannot send or receive new messages. Please delete some messages now." A similar message is displayed in the Cisco Unity Inbox.

  Additionally, when a subscriber mailbox reaches the Prohibit Send And Receive limit, ViewMail will not load when the subscriber starts Outlook. The ViewMail form cannot be published until the mailbox size is reduced.

For ways in which you and subscribers can manage subscriber mailbox size, see the "Best Practices for Managing Subscriber Mailbox Size" section in the "Configuring Cisco Unity for Maintenance Tasks" chapter of the *Maintenance Guide for Cisco Unity*.

For more information on Exchange 2000 and Exchange 2003 storage limits, see the "Setting a Maximum Size for Exchange Mailboxes" section in the "Configuring Exchange for Maintenance Tasks" chapter in the *Maintenance Guide for Cisco Unity*, or see the Microsoft Exchange documentation.

The *Maintenance Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

What Callers Experience When a Subscriber Mailbox Has Reached the Prohibit Send and Receive Limit

By default, Cisco Unity does not check whether a subscriber mailbox has exceeded the Prohibit Send and Receive limit before allowing a caller to leave a message, although Cisco Unity does check before sending the message to the subscriber mailbox. If the subscriber mailbox is no longer allowed to receive messages, Cisco Unity handles the message as follows:

- If the message was left by an unidentified caller, Cisco Unity sends the message to the Unaddressed Messages distribution list, which should be monitored by the Cisco Unity system administrator or another subscriber.

  Note that if the mailbox(es) of the subscriber(s) who are assigned to check the Unaddressed Messages list exceed the Prohibit Send and Receive storage limit that is specified in Exchange, the messages that are sent to the Unaddressed Messages distribution list are lost. To avoid this problem,

specify a generous value for the Prohibit Send and Receive storage limit for the mailbox of at least one subscriber who is a member of the Unaddressed Messages list, and encourage the subscriber to dispose of messages promptly so that the Exchange mailbox does not fill up.

- If the message was left by another subscriber, Cisco Unity sends a nondelivery receipt (NDR) message to the subscriber who left the message.

Cisco Unity can be set to check whether a subscriber mailbox has exceeded the Prohibit Send and Receive limit when an outside caller tries to leave a message for the subscriber. In this circumstance, when the mailbox is full, the outside caller hears the following prompt: "You cannot record a message for <Subscriber>. This mailbox is full." After playing the prompt, Cisco Unity transfers the caller back to the Opening Greeting and logs the following message to the Windows Application Event log: "The mailbox for [Alias: subscriber alias] is full. The subscriber cannot send or receive new voice messages until mailbox size is reduced. Mailbox size limits are specified in the message store, not Cisco Unity."

To enable Cisco Unity to check whether a subscriber mailbox is full when an outside caller tries to leave a message for the subscriber, you edit two registry keys:

- A key to allow you to specify that Cisco Unity will check whether a subscriber mailbox is full when an outside caller wants to leave a message.
- A key to allow you to enable or disable the prompt that informs callers that they cannot leave a message when the mailbox is full.

See the following "To Enable the Full-Mailbox Check and Prompt for Outside Callers" procedure for detailed instructions. Note that enabling full-mailbox checks for outside callers does not affect how Cisco Unity handles messages from other Cisco Unity subscribers to a full mailbox. Also, Cisco Unity behaves as if the full-mailbox check feature is disabled in the following circumstances:

- When an outside caller leaves a message for a call handler whose recipient is a distribution list (for example, the default recipient for the Operator call handler is the Unaddressed Messages list).
- When an outside caller leaves a message for an interview handler.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

To Enable the Full-Mailbox Check and Prompt for Outside Callers

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Full Mailbox Check Feature**.

Step 4 In the New Value list, click **1**, and then click **Set**.

Step 5 When prompted, click **OK**.

Step 6 In the Unity Settings pane, click **Conversation—Full Mailbox Check Prompt**.

Step 7 In the New Value list, click **1**, and then click **Set**.

Step 8 When prompted, click **OK**.

You do not need to restart Cisco Unity to enable the registry changes.

Step 9 Click **Exit**.

How Cisco Unity Handles Messages Without a Specific Recipient

In some situations, messages left in Cisco Unity are not associated with a specific recipient; these messages must be screened and routed to the applicable subscriber or call handler. A subscriber should be assigned the responsibility of reviewing these messages frequently.

Such messages are left as follows:

Unaddressed Messages Distribution List

Messages that cannot be delivered because the network or a server assigned to a subscriber goes down, or because the subscriber mailbox has exceeded the Prohibit Send and Receive limit specified for the mailbox in Exchange, are forwarded to the Unaddressed Messages distribution list. By default, this distribution list contains the Example Administrator as its only member.

To route these messages properly, ensure that the Unaddressed Messages distribution list has at least one member (such as the operator) who will monitor the mailbox and handle messages that cannot be delivered. (See the "To Add Subscribers to the Unaddressed Messages Distribution List" procedure on page 8-6 for instructions.)

Note that if the mailbox(es) of the subscriber(s) who are assigned to check the Unaddressed Messages list exceed the Prohibit Send and Receive storage limit that is specified in Exchange, the messages sent to the Unaddressed Messages distribution list are lost. To avoid this problem, specify a generous value for the Prohibit Send and Receive storage limit for the mailbox of at least one subscriber who is a member of the Unaddressed Messages list, and encourage the subscriber to dispose of messages promptly so that the Exchange mailbox does not fill up.

Operator, Opening Greeting, and Goodbye Call Handlers

When a caller to Cisco Unity dials the operator and no operator is available, the caller can leave a message, depending on the call transfer settings for the Operator call handler. Call transfer settings in the Opening Greeting and Goodbye call handlers also can allow callers to leave a message. By default, messages left in any of these call handlers are sent to the Unaddressed Messages distribution list.

Example Interview

When callers are routed to the Example Interview, which gathers basic information about who they are and who they are trying to reach, the answers to the questions are routed by default to the Example Administrator. If you want these messages to be routed to another recipient, choose a subscriber (such as the operator) or a distribution list as the recipient.

To Add Subscribers to the Unaddressed Messages Distribution List

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the **Unaddressed Messages** distribution list.

Step 4 Change settings as applicable, and then click the **Save** icon.

How Cisco Unity Handles Private Messages

Messages marked private cannot be forwarded by phone, from Cisco Unity ViewMail for Microsoft Outlook, or from the Cisco Unity Inbox. This includes any voice message that a Cisco Unity subscriber marked private, and as applicable, any e-mail message that a subscriber or another sender marked private in Outlook. In addition, when a message is marked private, the Copy and Copy To options are disabled on the Options menu on the Media Master control bar in ViewMail for Outlook and the Cisco Unity Inbox.

For subscribers who require more secure messaging, consider the following:

- You can set up secure messaging and enable subscribers to use it. Secure messaging provides security through the use of public/private key encryption for voice messages. Secure messages cannot be heard by anyone other than a Cisco Unity subscriber who is authenticated with their Cisco Unity server. For information on how to set up secure messaging, see the "Secure Messaging" section in the "Securing Subscriber Messages" 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.
- You can prevent subscribers from saving any voice message—regardless of its sensitivity—to their hard disks by disabling the Copy to File option on the Options menu of the Media Master control bar in the Cisco Unity Inbox. To learn more, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Disable Copy to File Option in Media Master). The Advanced Settings tool is available in Tools Depot.

How Cisco Unity Handles Messages That Contain Text

If your organization has both Voice Messaging and Unified Messaging subscribers, messaging between the two types of subscribers can be problematic. This is because Voice Messaging subscribers cannot use the Cisco Unity conversation or the Cisco Unity Inbox to access text in e-mail messages. In addition, when a message contains both a voice recording and a text message—as may be the case when a Unified Messaging subscriber uses Cisco Unity ViewMail for Microsoft Outlook to send, reply to, and forward messages to Voice Messaging subscribers, the Cisco Unity conversation and the Cisco Unity Inbox present only the voice portion of the message. Moreover, Cisco Unity informs neither the sender nor the recipient that all or a portion of a message is unavailable to the recipient.

You can set up Cisco Unity so that it rejects messages sent to Voice Messaging subscribers if the messages contain text. In this way, you can ensure that Voice Messaging subscribers receive only those messages that they can play in their entirety. At the same time, when Cisco Unity rejects messages that contain text, Unified Messaging subscribers receive a nondelivery receipt (NDR) and can learn to adjust their messaging habits accordingly.

For more information, see the following sections:

- Using the Message Store Manager to Change How Cisco Unity Handles Messages That Contain Text, page 8-8
- Understanding How Messages That Contain Text Are Handled After You Set Up Cisco Unity to Reject Them, page 8-8
- Task List for Setting Up Cisco Unity to Reject Messages That Are Sent to Voice Messaging Subscribers When the Messages Contain Text, page 8-11

Using the Message Store Manager to Change How Cisco Unity Handles Messages That Contain Text

The Message Store Manager utility allows you to set up agents that perform the task that you assign them to do. You specify which subscriber mailboxes are members of an agent; only the mailboxes that you specify are affected by the task performed by the agent.

To set up Cisco Unity so that it rejects messages that are sent to Voice Messaging subscribers, if the messages contain text, you need to create two agents:

- The first agent applies a rule that rejects messages that contain text. The agent applies the rule to the subscriber mailboxes that you specify as agent members. You can use a Cisco Unity distribution list, class of service, extension range, or an imported CSV file to specify agent members. However, we recommend that you use a distribution list or class of service, because as you add members to the distribution list or class of service, membership in the agent will be automatically updated at the same time.
- The second agent removes the rule that was applied by the first agent from subscriber accounts that no longer need it. Once the first agent is set up, it will continue to reject messages that contain text until the second agent removes it. If you do not set up the second agent, even after you remove a subscriber from the distribution list or class of service that you specified as a member of the first agent, the first rule will continue to reject messages from that subscriber mailbox if the messages contain text. We recommend that you set up both agents at the same time, setting the second agent to remove the rule from all subscriber mailboxes on the server except those that are associated with Voice Messaging subscribers. When the agents are set up this way, you will not have to create a new agent to remove the rule from a single mailbox each time that a Voice Messaging subscriber is removed from the distribution list or class of service that you specified for the first agent.

You schedule when and how often you want each agent to run. For example, you may choose to run the agents nightly or weekly, depending on how often you add or remove subscribers from the class of service or distribution list that you use to specify agent membership. As you determine a schedule for running the agents, consider that when Voice Messaging subscribers are set to not appear in the Outlook address books, the agents will take longer to run. Also note that while an agent is running, any previously hidden mailboxes appear in address books, and then, when the agent has completed its task, the mailboxes are hidden once again. For this reason, you may want to schedule the agents to run when subscribers are not likely to use the system. (Voice Messaging subscribers are often prevented from appearing in the Outlook address book as way of discouraging people from inadvertently sending e-mail messages to a Voice Messaging account.)

When you set up the agents, you can activate the Subscriber Message Store Status report (or you can schedule the report to run at a later time) to gather detailed data about each subscriber mailbox that is a member of the agent. When the value of the VM Mailbox Rule column equals one (1), the rule associated with the first agent has been applied; when the value equals zero (0), the rule has not been applied to the mailbox.

For more information on working with Message Store Manager to set up agents and run reports, see Message Store Manager Help.

Understanding How Messages That Contain Text Are Handled After You Set Up Cisco Unity to Reject Them

When you set up Cisco Unity so that it rejects messages sent to Voice Messaging subscribers when the messages contain text, Voice Messaging subscribers continue to receive receipts, faxes, and voice messages as before, but many other types of messages are no longer delivered. Knowing how Cisco Unity handles messages differently can help you prepare both Voice Messaging and Unified Messaging subscribers for the change.

Table 8-1 compares how Cisco Unity handles messages by default, to how Cisco Unity handles messages after you have set it to reject messages that are sent to Voice Messaging subscribers when the messages contain text. Keep in mind that when Cisco Unity rejects a message, it does so when the Voice Messaging subscriber is the sole recipient of the message, and also when the subscriber is one of many recipients, as may be the case when a message containing text is sent to a distribution list. Note that in a few cases, Cisco Unity does not reject certain types of messages that you may expect, while it rejects others that you may not expect.

Table 8-1 How Messages That Contain Text Are Handled When Sent to Voice Messaging Subscriber

Type of Message	Application Used to Send Message	How Cisco Unity Handles Message by Default	How Cisco Unity Handles Messages When Set Up to Reject Messages That Contain Text
Voice message with text in subject line	ViewMail	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Does not deliver message; sends an NDR to sender.
Voice message with text in subject line	Cisco Unity Inbox	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Same as default.
Voice message with text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Voice message with a non-WAV attachment	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access the attachment.	Does not deliver message; sends an NDR to sender.
Reply to voice message with voice recording and text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Reply to voice message with text in message body	ViewMail	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.
Reply to voice message with non-WAV attachment	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access the attachment.	Does not deliver message; sends an NDR to sender.
Reply to voice message with no voice recording, no change to subject line, and no text in message body	ViewMail	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.
Reply to voice message with change to text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Reply to voice message with change to subject line	ViewMail	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Does not deliver message; sends an NDR to sender.

Table 8-1 How Messages That Contain Text Are Handled When Sent to Voice Messaging Subscriber (continued)

Type of Message	Application Used to Send Message	How Cisco Unity Handles Message by Default	How Cisco Unity Handles Messages When Set Up to Reject Messages That Contain Text
Reply to voice message with change to subject line	Cisco Unity Inbox	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Same as default.
Reply to voice and text message with voice recording and deletion of all text	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Same as default.
Reply to voice and text message with voice recording	Cisco Unity conversation	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Reply to voice and text message with voice recording	Cisco Unity Inbox or ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Same as default.
Reply to e-mail message with voice recording and text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Reply to e-mail message with voice recording	Cisco Unity conversation or ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Same as default.
Reply to e-mail message with text in message body	ViewMail	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with voice introduction and text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with non-WAV attachment	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access the attachment.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with change to text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with change to subject line	ViewMail	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Does not deliver message; sends an NDR to sender.
Forwarded voice message with change to subject line	Cisco Unity Inbox	Delivers message as voice message; Voice Messaging subscribers can access subject line only in Cisco Unity Inbox.	Same as default.

Table 8-1 How Messages That Contain Text Are Handled When Sent to Voice Messaging Subscriber (continued)

Type of Message	Application Used to Send Message	How Cisco Unity Handles Message by Default	How Cisco Unity Handles Messages When Set Up to Reject Messages That Contain Text
Forwarded voice and text message with or without voice introduction	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Same as default.
Forwarded voice and text message with or without voice introduction	Cisco Unity conversation or the Cisco Unity Inbox	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Forwarded voice and text message with deletion of all text	ViewMail	Delivers message as voice message.	Same as default.
Forwarded e-mail with text in message body	ViewMail	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.
Forwarded e-mail message with voice introduction and text in message body	ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Does not deliver message; sends an NDR to sender.
Forwarded e-mail message with voice introduction	Cisco Unity conversation or ViewMail	Delivers message as voice message; Voice Messaging subscribers cannot access text.	Same as default.
Forwarded e-mail message with no change to subject line or additional text	Cisco Unity conversation or ViewMail	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.
E-mail message with WAV attachment	E-mail program	Delivers message as e-mail message that Voice Messaging subscribers cannot access; Voice Messaging subscribers cannot access the attachment.	Does not deliver message; sends an NDR to sender.
E-mail message	E-mail program	Delivers message as e-mail message that Voice Messaging subscribers cannot access.	Does not deliver message; sends an NDR to sender.

Task List for Setting Up Cisco Unity to Reject Messages That Are Sent to Voice Messaging Subscribers When the Messages Contain Text

Complete the following tasks to set up Cisco Unity so that it rejects messages that are sent to Voice Messaging subscribers when the messages contain text:

1. Identify the Voice Messaging subscribers on your Cisco Unity server. For example, create a class of service or public distribution list for Voice Messaging subscribers, and then use the Cisco Unity Administrator or Bulk Edit to assign the appropriate subscribers to it. (Note that how you differentiate Voice Messaging subscribers from Unified Messaging subscribers is up to you; nothing in the way that you created them, nor in how they are licensed, identifies them as Voice Messaging or Unified Messaging subscribers for this feature.)

2. Set up the two agents that will enable Cisco Unity to reject messages that are sent to Voice Messaging subscribers when the messages contain text. See the "To Set Up an Agent to Reject Messages That Contain Text When the Messages Are Sent to Voice Messaging Subscribers" procedure on page 8-13 and the "To Set Up an Agent to Ensure Unified Messaging Subscribers Receive Messages That Contain Text" procedure on page 8-13.
3. Customize ViewMail for Outlook so that when it is installed on subscriber workstations, messages that are sent to Voice Messaging subscribers are checked for text. You need to do this even if you are upgrading subscriber workstations from a customized version of ViewMail 4.1(1) to ViewMail 4.2(1). See the "To Customize ViewMail for Outlook Version 4.1(1) and Later to Check for Text When Subscribers Send Messages to Voice Messaging Subscribers" procedure on page 8-14.
4. Install the customized version of ViewMail on all subscriber workstations. See the "To Install the Customized Version of ViewMail on All Subscriber Workstations" procedure on page 8-14.

Note If you already installed a standard version of ViewMail on subscriber workstations, you cannot simply install the customized version of ViewMail to enable the feature. You also cannot repair the existing installation to enable the feature. To enable the feature if you already installed a standard version of ViewMail, you must change the value of a registry key to 1 on each subscriber workstation. The registry key is HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\Cisco Unity\VMO\NoTextToVM. It is a DWORD key. You can edit the registry on each subscriber workstation, or you can use a software publishing tool to update the key value on all subscriber workstations at once.

5. Subscribers who use Microsoft Outlook 2002 and later will get a Microsoft Outlook security alert when they use the customized version of ViewMail. Tell subscribers that they can safely click Yes in response. The standard text for the security alert informs users that an application is attempting to access the Outlook Address Book, and asks them if they want to allow it. (In fact, ViewMail does not access the Address Book, but it does check for text in each message that triggers the alert.) To learn more about the Microsoft Outlook Security feature—as well as how to customize or disable it, see the Microsoft Office Assistance topic "Customizing the Outlook Security Features Administrative Package," in the "Administering Outlook Security" chapter of the Messaging Deployment Guide on the Microsoft website.
6. Consider letting subscribers know what to expect now that Cisco Unity rejects messages sent to Voice Messaging subscribers when the messages contain text. Give everyone a list of Voice Messaging subscribers so that they know which subscribers cannot receive messages that contain text. In addition, tell Unified Messaging subscribers that if they receive an NDR in response to a message that they sent to a Voice Messaging subscriber, they should remove all text before attempting to resend the message. Remind them that NDRs can also be triggered when a recipient has a full mailbox.

Note When you move a Voice Messaging subscriber mailbox from one Exchange server to another, the rules associated with the mailbox continue to work after the move. The same is true when you move a Voice Messaging subscriber from one Cisco Unity server to another. If the other Cisco Unity server is not already set up to reject messages that contain text, consider enabling it so that messages to Voice Messaging subscribers are handled consistently. Alternatively, you can create a new agent to remove the rule from the individual mailbox before moving the subscriber to the other Cisco Unity server.

To Set Up an Agent to Reject Messages That Contain Text When the Messages Are Sent to Voice Messaging Subscribers

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Message Store Manager**.

Step 3 From the File menu, click **New Agent**.

Step 4 Enter a name for the agent, then click **OK**. For example, consider naming the agent, "Reject Text to VM Subscribers."

Step 5 Right-click the **Included** folder, and click the option that allows you to specify that only Voice Messaging subscribers are members of the agent. For example, if you created a class of service to identify Voice Messaging subscribers on your server, you would click Add Class of Service.

Step 6 Click the applicable class of service or distribution list, then click **OK**.

Step 7 Click the **Scripts** directory.

Step 8 From the list displayed in the right pane, right-click **Add VM Mailbox Rules** and click **Activate**.

Step 9 In the MSM Script dialog box, click the **Schedule** tab. Specify how often you want the agent to run.

Note The agent takes longer to run if any members are currently hidden from Outlook address books.

Step 10 Click **OK** to close the MSM Script dialog box.

To Set Up an Agent to Ensure Unified Messaging Subscribers Receive Messages That Contain Text

Step 1 From the File menu, click **New Agent**.

Step 2 Enter a name for the agent, then click **OK**. For example, consider naming the agent, "Remove VM Subscribers Rule."

Step 3 Right-click the **Included** folder, and click the option that allows you to specify all subscribers as members of the agent. For example, if you have an All Subscribers distribution list, you would click Add Distribution List.

Step 4 Click the applicable class of service or distribution list, then click **OK**.

Step 5 Right-click the **Excluded** folder, and click the option that allows you to specify that Voice Messaging subscribers are excluded as members of the agent. For example, if you created a class of service to identify Voice Messaging subscribers, you would click Add Class of Service.

Step 6 Click the applicable class of service or distribution list, then click **OK**.

Step 7 Click the **Scripts** directory.

Step 8 From the list displayed in the right pane, right-click **Delete VM Mailbox Rules** and click **Activate**.

Step 9 In the MSM Script dialog box, click the **Schedule** tab and specify how often you want the agent to run.

Note The agent takes longer to run if any members are currently hidden from Outlook address books.

Step 10 Click **OK** to close the MSM Script dialog box.

To Customize ViewMail for Outlook Version 4.1(1) and Later to Check for Text When Subscribers Send Messages to Voice Messaging Subscribers

Step 1 Download ViewMail or browse to the ViewMail directory on the Cisco Unity DVD, as applicable. See the applicable *Release Notes for Cisco Unity ViewMail for Microsoft Outlook* for the version of ViewMail that you are customizing. The document is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Step 2 In the ViewMail directory, browse to the ENU language folder.

Step 3 Open the **VMOInit.VBS** file in a text editor such as Notepad.

Step 4 Enter **Session.Property("NOTEXTTOVM") = "1"** immediately before the End Function line, as shown below:

```
Function VMOInitFn()
rem Session.Property("EXTENSION") = ""
rem Session.Property("UNITYSERVER") = ""
Session.Property("NOTEXTTOVM") = "1"
End Function
```

Step 5 Save the script file and close the text editor.

Step 6 Open a Command Prompt window. (On the Windows Start menu, click **Programs > Accessories > Command Prompt**.)

Step 7 Change to the **ViewMail > ENU** directory.

Step 8 Enter **vmaddbin ViewMail.MSI VMOInit.VBS**, and press **Enter**. (When the script completes, your cursor returns to the command line.)

Step 9 Close the Command Prompt window.

To Install the Customized Version of ViewMail on All Subscriber Workstations

Step 1 For the version of ViewMail that you customized in the "To Customize ViewMail for Outlook Version 4.1(1) and Later to Check for Text When Subscribers Send Messages to Voice Messaging Subscribers" procedure on page 8-14, review the applicable *Release Notes for Cisco Unity ViewMail for Microsoft Outlook* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html for requirements, installation instructions, and other important information.

Step 2 By using the ViewMail.msi file that you customized, install ViewMail on all subscriber workstations.

You can install ViewMail by using any of the methods described in the applicable *Release Notes for Cisco Unity ViewMail for Microsoft Outlook*.

CHAPTER 9

Managing Account Policy Settings

See the following sections in this chapter:

Account Policy Settings Overview

The account policy settings on the Phone Password Restrictions Page and the Cisco Unity Account Lockout Page in the Cisco Unity Administrator apply when subscribers access Cisco Unity by phone. Changes to settings in the account policy affect all existing subscribers.

Note that the settings on the Account Policy pages represent a different account policy from the one that applies when subscribers use web applications to access Cisco Unity. For information on specifying an account policy for the Cisco Personal Communications Assistant (PCA) and the Cisco Unity Administrator, see the "Authentication Settings" section on page 11-1.

Phone Password Restriction Settings

Phone password restriction settings allow you to define a system-wide password policy that applies when subscribers access Cisco Unity by phone. For greater security, establish rules that prevent passwords from being easy to guess and from being used for a long time. At the same time, is also best to avoid requiring passwords that are so complicated or that must be changed so often that subscribers have to write them down to remember them. Consider requiring that subscribers use a long—eight or more digits—and non-trivial password when you specify phone password restrictions.

Phone password restrictions cannot be changed for individual subscriber accounts. However, you can use the password settings on the template and on individual subscriber pages in the Cisco Unity Administrator to govern the passwords that subscribers initially use to log on to Cisco Unity by phone, and to define whether and when subscribers can change their own phone passwords. You can also use the Cisco Unity Bulk Import wizard to set phone passwords for multiple subscriber accounts at the same time. (See Cisco Unity Bulk Import Help for details.)

Account Lockout Settings

Cisco Unity account lockout settings allow you to specify whether you want Cisco Unity to use an account lockout policy that applies to all subscribers who access Cisco Unity by phone. To customize the account lockout policy for your organization, you can use the settings on the Cisco Unity Account Lockout page to dictate:

- How Cisco Unity handles situations when subscribers attempt to log on to Cisco Unity by phone and repeatedly enter incorrect phone passwords.
- The number of failed logon attempts that are allowed before Cisco Unity prohibits the subscriber from accessing Cisco Unity by phone.
- The length of time that a subscriber who is locked out must wait before attempting to access Cisco Unity by phone again.

Changes to account policy settings affect all Cisco Unity subscribers. You cannot change account policy settings for individual subscriber accounts, though you can lock individual subscriber accounts to prevent subscribers from using the phone to access Cisco Unity.

CHAPTER 10

Managing Languages

The Cisco Unity Administrator provides settings for phone languages, Text to Speech (TTS), and GUI languages. Phone languages are the languages in which Cisco Unity plays system prompts to subscribers and callers; TTS languages are the languages in which Cisco Unity plays e-mail messages over the phone, and GUI languages are the languages in which the Cisco Unity Administrator is displayed.

The number of language licenses available determines how many phone, TTS, and GUI languages Cisco Unity can load and use at a time. For example, if your organization has two phone language licenses, but has four languages installed, Cisco Unity will allow you to load and use only two at any one time. You can, however, select which two are used, and you can change this selection at any time. This flexibility allows you to better manage the language needs of your users.

For the complete list of supported languages for Cisco Unity, see the "Available Languages for Cisco Unity Components" section of the applicable *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Customizing system prompts is not supported for any of the Cisco Unity phone languages. All system prompts are automatically deleted and replaced when you upgrade Cisco Unity, including the installation of maintenance releases.

See the following sections in this chapter:

Languages Overview

The phone, TTS, and GUI languages are chosen and installed during the initial Cisco Unity setup, and the applicable files are copied to the Cisco Unity server for each selected language.

One of the languages installed on the Cisco Unity server must match the Windows locale selected during Windows installation. Additional languages may be installed as needed.

If during initial setup you did not install the language(s) you need, see the "Adding Languages" section in the "Adding Features to the Cisco Unity System" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity* for details on how to add or replace languages. If you are adding TTS, see the "Adding Text to Speech" section. (The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)

Caution Before removing a Cisco Unity language, confirm that it is not the language that matches the Windows locale, that it is not listed in the Loaded table on the System > Configuration > Phone Languages and/or GUI Languages pages, that it is not listed as the default Phone, TTS, or GUI language, and that it is not in use by any subscriber, routing rule, call handler, interview handler, or directory handler. Do not change the Windows locale language without updating all of the locations where the corresponding Cisco Unity languages (both old and new) are specified.

In the following circumstances, if the language specified is not listed in the Loaded table on the System > Configuration > Phone Languages and/or GUI Languages pages, Cisco Unity will use the default phone, TUI, or GUI language:

- When a language is specified in a Cisco Unity component
- When a language is specified as the Windows locale
- When a language is passed to Cisco Unity by the Property Management System (for Hospitality integrations)

If you have a Cisco Unity failover system, languages settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

Specifying Text to Speech Languages

The Text to Speech (TTS) language engine translates e-mail text into audio, enabling subscribers to listen to e-mail by using the phone. TTS is available only with Unified Messaging and only to subscribers who have class of service rights to use it. (Note that even those who do not have class of service rights to TTS will hear e-mail messages announced when they review messages in their Deleted Items folder, as applicable. The e-mails are not read to subscribers; Cisco Unity announces each e-mail and subscribers are offered the opportunity to delete it, mark it new, and so on.)

The default TTS language is specified during installation, and can be viewed and changed on the System > Configuration > Phone Languages page.

The Cisco Unity server can support multiple TTS language engines. However, subscribers are limited to choosing one of the loaded languages, as multiple TTS languages are not supported on an individual subscriber basis. For example, a subscriber who receives one message in French and another message in Italian will hear both messages in the TTS language that corresponds to the selected phone language.

All supported TTS language engines are automatically installed with the Cisco Unity software.

Use of TTS is controlled by the number of Text to Speech session licenses, and by subscriber class of service. The number of simultaneous TTS sessions on a Cisco Unity server cannot exceed the maximum number of sessions supported for the applicable platform overlay, as specified in the *Cisco Unity Supported Platforms List* (available at http://www.cisco.com/warp/public/cc/pd/unco/un/prodlit/ucutp_st.htm). Depending on the needs of your site, you can grant TTS use to all subscriber classes of service, or limit it to specific classes of service.

Typically, the phone language(s) that you install and choose for use by subscribers will also be used as their TTS language(s), with the following exceptions:

- If you installed Arabic, Australian English, Canadian English, Czech, Hungarian, Polish, New Zealand English, Russian, or TTY English as your phone language during setup, the language installed for the Cisco Unity Administrator GUI language is used as the default TTS language.

- Chinese-PRC, Chinese-Taiwan, Chinese-Hong Kong SAR, Japanese, and Korean TTS require specific language settings on the Cisco Unity server. If you are using any of these languages, complete the procedures in the following "Using Chinese-PRC, Chinese-Taiwan, Chinese-Hong Kong SAR, Japanese, and Korean Text to Speech" section, as applicable.

Using Chinese-PRC, Chinese-Taiwan, Chinese-Hong Kong SAR, Japanese, and Korean Text to Speech

Complete the applicable procedure in this section to set up the Cisco Unity server to use Chinese-PRC, Chinese-Taiwan, Chinese-Hong Kong SAR, Japanese, and Korean TTS.

Procedures for a Cisco Unity Server Running Windows 2000

- To Use Chinese-PRC Text to Speech on a Windows 2000 Server, page 10-3
- To Use Chinese-Taiwan Text to Speech on a Windows 2000 Server, page 10-3
- To Use Chinese-Hong Kong SAR Text to Speech on a Windows 2000 Server, page 10-4
- To Use Japanese Text to Speech on a Windows 2000 Server, page 10-4
- To Use Korean Text to Speech on a Windows 2000 Server, page 10-4

Procedures for a Cisco Unity Server Running Windows 2003

- To Use Chinese-PRC Text to Speech on a Windows 2003 Server, page 10-5
- To Use Chinese-Taiwan Text to Speech on a Windows 2003 Server, page 10-5
- To Use Chinese-Hong Kong SAR Text to Speech on a Windows 2003 Server, page 10-5
- To Use Japanese Text to Speech on a Windows 2003 Server, page 10-5
- To Use Korean Text to Speech on a Windows 2003 Server, page 10-6

To Use Chinese-PRC Text to Speech on a Windows 2000 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional Options**.

Step 2 On the General tab, in the Your Locale (Location) list, click **Chinese (PRC)**.

Step 3 In the Language Settings for the System box, click **Simplified Chinese**.

If you have a multi-lingual system, choose additional languages as applicable.

Step 4 Click **Set Default**. The Set System Locale dialog box opens.

Step 5 In the Select Appropriate Locale list, click **Chinese (PRC)**.

Step 6 Restart the Cisco Unity server for the changes to take effect.

To Use Chinese-Taiwan Text to Speech on a Windows 2000 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional Options**.

Step 2 On the General tab, in the Your Locale (Location) list, click **Chinese (Taiwan)**.

Step 3 In the Language Settings for the System box, click **Traditional Chinese**.

If you have a multi-lingual system, choose additional languages as applicable.

Step 4 Click **Set Default**. The Set System Locale dialog box opens.

Step 5 In the Select Appropriate Locale list, click **Chinese (Taiwan)**.

Step 6 Restart the Cisco Unity server for the changes to take effect.

To Use Chinese-Hong Kong SAR Text to Speech on a Windows 2000 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional Options**.

Step 2 On the General tab, in the Your Locale (Location) list, click **Chinese (Hong Kong)**.

Step 3 In the Language Settings for the System box, click **Traditional Chinese**.

If you have a multi-lingual system, choose additional languages as applicable.

Step 4 Click **Set Default**. The Set System Locale dialog box opens.

Step 5 In the Select Appropriate Locale list, click **Chinese (Hong Kong)**.

Step 6 Restart the Cisco Unity server for the changes to take effect.

To Use Japanese Text to Speech on a Windows 2000 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional Options**.

Step 2 On the General tab, in the Your Locale (Location) list, click **Japanese**.

Step 3 In the Language Settings for the System box, click **Japanese**.

If you have a multi-lingual system, choose additional languages as applicable.

Step 4 Click **Set Default**. The Set System Locale dialog box opens.

Step 5 In the Select Appropriate Locale list, click **Japanese**.

Step 6 Restart the Cisco Unity server for the changes to take effect.

To Use Korean Text to Speech on a Windows 2000 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional Options**.

Step 2 On the General tab, in the Your Locale (Location) list, click **Korean**.

Step 3 In the Language Settings for the System box, click **Korean**.

If you have a multi-lingual system, choose additional languages as applicable.

Step 4 Click **Set Default**. The Set System Locale dialog box opens.

Step 5 In the Select Appropriate Locale list, click **Korean**.

Step 6 Restart the Cisco Unity server for the changes to take effect.

To Use Chinese-PRC Text to Speech on a Windows 2003 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional and Language Options**.

Step 2 On the Languages tab, confirm that the **Install Files for East Asian Languages** check box is checked.

Step 3 On the Regional Options tab, in the drop-down menu for the Standards and Formats section, click **Chinese (PRC)** from the list.

Step 4 In the Location section, click **China**.

Step 5 On the Advanced tab, in the Language For Non-Unicode Programs section, click **Chinese (PRC)**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server for the changes to take effect.

To Use Chinese-Taiwan Text to Speech on a Windows 2003 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional and Language Options**.

Step 2 On the Languages tab, confirm that the **Install Files for East Asian Languages** check box is checked.

Step 3 On the Regional Options tab, in the drop-down menu for the Standards and Formats section, click **Chinese (Taiwan)** from the list.

Step 4 In the Location section, click **Taiwan**.

Step 5 On the Advanced tab, in the Language For Non-Unicode Programs section, click **Chinese (Taiwan)**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server for the changes to take effect.

To Use Chinese-Hong Kong SAR Text to Speech on a Windows 2003 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional and Language Options**.

Step 2 On the Languages tab, confirm that the **Install Files for East Asian Languages** check box is checked.

Step 3 On the Regional Options tab, in the drop-down menu for the Standards and Formats section, click **Chinese (Hong Kong SAR)** from the list.

Step 4 In the Location section, click **Hong Kong SAR**.

Step 5 On the Advanced tab, in the Language For Non-Unicode Programs section, click **Chinese (Hong Kong SAR)**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server for the changes to take effect.

To Use Japanese Text to Speech on a Windows 2003 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional and Language Options**.

Step 2 On the Languages tab, confirm that the **Install Files for East Asian Languages** check box is checked.

Step 3 On the Regional Options tab, in the drop-down menu for the Standards and Formats section, click **Japanese** from the list.

Step 4 In the Location section, click **Japan**.

Step 5 On the Advanced tab, in the Language For Non-Unicode Programs section, click **Japanese**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server for the changes to take effect.

To Use Korean Text to Speech on a Windows 2003 Server

Step 1 On the Windows Start menu, click **Settings > Control Panel > Regional and Language Options**.

Step 2 On the Languages tab, confirm that the **Install Files for East Asian Languages** check box is checked.

Step 3 On the Regional Options tab, in the drop-down menu for the Standards and Formats section, click **Korean** from the list.

Step 4 In the Location section, click **Korea**.

Step 5 On the Advanced tab, in the Language For Non-Unicode Programs section, click **Korean**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server for the changes to take effect.

Phone Language Settings

Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers. You specify a default phone language and other system-wide phone language settings, as well as the default Text to Speech (TTS) language, which is the language that subscribers hear when their e-mail is read to them over the phone. Note that to use TTS languages, your organization must have TTS e-mail and the applicable languages installed. See the "Languages Overview" section on page 10-1 for more information about using multiple languages.

You can customize the language settings for specific Cisco Unity components such as subscriber accounts, routing rules, call handlers, interview handlers, and directory handlers.

Specifying Phone Languages

Caution If you have a Cisco Unity failover system, phone languages settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

You specify a default phone language and other system-wide phone language settings on the System > Configuration > Phone Languages page.

You can customize the language setting for individual Cisco Unity components without changing the default language settings for the rest of the system. The phone language setting is available for the following Cisco Unity components: subscriber accounts, routing rules, call handlers, interview handlers, and directory handlers. For each of these entities, you can use the pages in the Cisco Unity Administrator to specify a phone language, or you can specify that the phone language be "Inherited."

With the Inherited setting, Cisco Unity determines the phone language to use for callers on a per-call basis, depending on how the call is processed. For example, you can set up a call handler with the Inherited language setting, and also set it up to receive calls from two different routing rules, each with a different language setting. (For example, one routing rule could be set up with a French language setting, while the second routing rule could be set to German.) In this situation, the language in which Cisco Unity plays the call handler system prompts will depend on which rule routed the call. However, note that if every component in your system that processes a call has been set with Inherited as the language setting, Cisco Unity will play the system prompts in the default phone language, because in effect none of the components will have been set to a specific language.

Recorded greetings are always played in the language in use when the greeting was recorded. For example, changing the language setting for the Opening Greeting call handler from U.S. English to French will not automatically convert the greeting that was originally recorded in English to one that is played back in French. The Opening Greeting must be re-recorded in French. This is also true for subscriber greetings and for other handlers.

Do the following "To Change Phone Language Settings for Cisco Unity Components" procedure to change the phone language settings for routing rules, call handlers, interview handlers, and directory handlers.

To specify phone language settings for individual subscribers, do the "To Change Phone Language Settings for Subscriber Accounts" procedure on page 10-8. To modify language settings for multiple subscriber accounts, you can use the Cisco Unity Bulk Import wizard or the Bulk Edit utility. Note that subscribers can use the Cisco Unity Assistant to select the language that they hear when they log on to Cisco Unity by phone.

To Change Phone Language Settings for Cisco Unity Components

Step 1 In the Cisco Unity Administrator, go to the applicable Call Routing, Call Handler, Interview Handler, or Directory Handler page.

Step 2 Go to following page(s), as applicable:

- For routing rules, go to the **Direct Calls** page or **Forwarded Calls** page.
- For call handlers, go to the **Profile** page.
- For interview handlers, go to the **Profile** page.
- For directory handlers, go to the **Profile** page.

Step 3 In the Language field, select one of the languages listed, or select **Inherited**.

Step 4 Re-record applicable greetings in the new language.

To Change Phone Language Settings for Subscriber Accounts

For each subscriber account, you can specify the language in which system prompts are played to callers (this affects prompts such as "Record your message at the tone"), and you can change the language that subscribers hear when listening to the subscriber conversation.

Note that if the class of service to which a subscriber belongs has TTS, the language you select in the Subscriber's Language field also controls the language that the TTS e-mail reader uses. Before changing the phone and TTS language for a subscriber, verify that you have the applicable languages installed.

Step 1 In the Cisco Unity Administrator, go to any **Subscriber** page.

Step 2 Do the following actions, as applicable:

- To change the phone language for callers, go to the **Messages** page. In the Language That Callers Hear field, select a specific language, or select **Inherited**.
- To change the phone language for subscribers, go to the **Conversation** page. In the Subscriber's Language field, select one of the languages listed.

Step 3 Ask the subscriber to re-record their greeting(s) in the new language.

GUI Languages Settings

The settings on the GUI Languages page determine the languages in which the Cisco Unity Administrator pages can be displayed. You specify a default GUI language and other system-wide GUI language settings.

To change the GUI language used in the Cisco Unity Administrator or the Cisco Personal Communications Assistant (PCA), select a language in the browser. (Subscribers use the Cisco PCA website to access the Cisco Unity Assistant and the Cisco Unity Inbox.)

For the Cisco Unity Administrator, note that the language selected in the browser must be one of the languages in the Loaded list on the GUI Languages page. If the language that you select in the browser is not among the loaded languages, Cisco Unity uses the default GUI language. For the Cisco PCA, the language selected in the browser must be one of the languages that the Cisco PCA offers.

Specifying GUI Languages

Caution If you have a Cisco Unity failover system, GUI languages settings are not replicated between the primary and secondary servers. You must change values manually on both servers.

You specify a default GUI language and other system-wide GUI language settings on the System > Configuration > GUI Languages Page. To change the GUI language used in the Cisco Unity Administrator and the Cisco PCA, select a language in the browser.

TTY Overview

A TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call in to Cisco Unity and use the same features that a hearing caller can use. However, note the following limitations:

- G.711 MuLaw must be selected as the message recording and storage codec. The Cisco Unity TTY prompt set is not compatible with G.729a or other message recording and storage codecs.
- A dedicated phone number must be set up for use by outside callers with TTY. All greetings, prompts, and subscriber names accessible from this number must be created with the TTY prompt set.
- TTY is a TUI language only. At the present time, there is no compatible Text to Speech (TTS) language for TTY. The TTY prompt set is also not suitable for use as a GUI language.
- TTY tones are not available for use in navigating through the Cisco Unity conversation. Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.
- Due to recording and playback limitations, the TTY prompt set can not be used in interview handlers.

See the following sections for information on setting up and using the Cisco Unity TTY prompt set:

- Setting Up Cisco Unity to Use the TTY Prompt Set, page 10-9
- Disabling Cisco Unity Comfort Noise, page 10-10
- Using the TTY Angel, page 10-11
- Using NTS for Advanced TTY Features, page 10-11

Setting Up Cisco Unity to Use the TTY Prompt Set

To set up Cisco Unity for TTY, do the following tasks.

1. Obtain a dial-in number that will be used exclusively for outside callers with TTY to call in to Cisco Unity. Set up the phone system and integration as required.
2. Install TTY devices for subscribers, as needed.
3. Install the ENX language on the Cisco Unity server.
4. Confirm that G.711 is selected as the Cisco Unity message recording and storage code.
5. Disable Cisco Unity comfort noise. See the "Disabling Cisco Unity Comfort Noise" section on page 10-10.
6. Create a TTY subscriber template. This template will be used when creating subscriber accounts for all subscriber who will use TTY. You may also want to create a TTY class of service, on which you disable Text to Speech for these subscribers.
7. Create a routing rule for the TTY dial-in number.
8. Create an opening greeting call handler for the TTY dial-in number.
9. Set up additional TTY call handlers as needed.

10. Record greetings in TTY by using the TTY Angel, or by using the Media Master and a TTY phone as a recording and playback device. You will need to record the following greetings, as applicable: the opening greeting, additional call handler greetings, and subscriber greetings. See the "Using the TTY Angel" section on page 10-11.
11. Test the TTY dial-in number, opening greeting, call handlers, and all subscriber devices to confirm correct operation for both incoming and outgoing TTY calls.

Disabling Cisco Unity Comfort Noise

Comfort noise is low-level background noise generated on a IP device. Its purpose is to simulate the hiss produced in a circuit-switched connection, and it can be generated to help provide reassurance to callers when there is no audio from Cisco Unity, for example, during a transfer or between system prompts.

The Cisco Unity ComfortNoise registry setting is a system-wide setting that controls the ability of Cisco Unity to send comfort noise generation packets to an IP phone, or to a gateway that is enabled to receive and respond to comfort noise generation packets.

If Cisco Unity comfort noise is enabled on a system that is using the TTY prompt set, TTY subscribers may report that characters are occasionally garbled or dropped. Disabling Cisco Unity comfort noise will prevent this problem from occurring.

Disabling Cisco Unity comfort noise should not cause a problem for non-TTY subscribers, but be aware that callers may notice short periods of silence between some Cisco Unity prompts.

To Disable Cisco Unity Comfort Noise

Step 1 Start **Regedit**.

Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the "Restoring" topics in Registry Editor Help.) Note that for a Cisco Unity failover system, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated. If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3 Expand the registry key

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Avaudio\Parameters\ComfortNoise

Step 4 In the Edit Dword Value window, click **Decimal**.

Step 5 Set the value to **128**.

Step 6 Click **OK**.

Step 7 Restart the Cisco Unity server.

Step 8 If you are using failover, repeat this procedure to apply the registry setting to secondary server.

Using the TTY Angel

The TTY prompt set includes all system prompts needed to use TTY with Cisco Unity. The TTY Angel application, available in Tools Depot, is used to create custom call handler and subscriber greetings, and subscriber recorded names, in TTY.

You can also create a CSV file containing a list of greetings and subscriber names to be converted to TTY all at once. See TTY Angel Help for more information about this option.

To Use the TTY Angel to Create Greetings and Recorded Names

Step 1 On the Cisco Unity desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, expand **Administrative Tools**, and double-click **TTY Angel**. The TTY Angel window appears.

Step 3 To create a new greeting or subscriber voice name, in the Output File Name window, enter a location and file name for the new TTY file.

For example, enter C:\TTY Greetings\Opening Greeting.

Step 4 In the Text to Convert to TTY/TDD WAV File window, enter the greeting, subscriber name, or other text as applicable, and click **Create WAV File**.

The text is converted, displayed in the Diagnostic Output window, and stored in the designated output file and in the clipboard.

Step 5 To paste the TTY WAV file into a call handler or subscriber record, in the Cisco Unity Administrator, browse to the applicable subscriber or call handler page.

Step 6 On the Media Master Control Bar, click the **Options** menu, and click **Paste** or **Paste From File** as applicable. The WAV file is pasted into the record.

Using NTS for Advanced TTY Features

NTS version 4.0 and later, available from NXi Communications, is compatible with Cisco Unity and Cisco Unified CM. NTS offers advanced TTY features for business and individual use.

CHAPTER 11

Managing System-Wide Settings

See the following sections in this chapter:

Authentication Settings

Authentication settings dictate the logon and lockout policy that applies when subscribers access Cisco Unity by using the Cisco Personal Communications Assistant (PCA). If the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method, the policy that you specify on the System > Authentication page also applies when subscribers use the Cisco Unity Administrator or the Status Monitor to access Cisco Unity.

Changes to authentication settings affect all Cisco Unity subscribers. You cannot change authentication settings for individual subscriber accounts, though you can lock out individual subscriber accounts to prevent subscribers from using the Cisco PCA, the Cisco Unity Administrator, or the Status Monitor to access Cisco Unity.

Related Documentation

- To understand how authentication works with Cisco Unity web applications, see the "Authentication for Cisco Unity Applications" chapter of the *Security Guide for Cisco Unity*.
- Consider that when subscribers log on to the Cisco PCA, their credentials are sent across the network to Cisco Unity in clear text. The same is true if the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method. For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. See the "Using SSL to Secure Client/Server Connections" chapter of the *Security Guide for Cisco Unity*.

The *Security Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Note that authentication settings represent a different logon and lockout policy from the one that applies when subscribers access Cisco Unity by phone. For information on setting up the account policy that applies when subscribers access Cisco Unity by phone, see the "Managing Account Policy Settings" chapter.

Voice Messaging Port Settings

Each voice messaging port on the Cisco Unity server can be set to perform one or more of these functions:

- Answer incoming calls from unidentified callers and from subscribers dialing in to Cisco Unity.
- Dial out to notify subscribers of voice, fax, and e-mail messages.
- Dial out to allow system administrators and subscribers to use the phone as a recording and playback device in Cisco Unity applications. (The phone is offered as a recording and playback device in the Media Master, which appears on pages of the Cisco Unity Administrator, Cisco Unity Assistant, and Cisco Unity Inbox, and in ViewMail.)

  You can adjust the maximum number of rings that Cisco Unity waits for when making these dial-out calls. See the Advanced Settings tool Help (in the Unity Settings list, click Administration—Set Maximum Number of Rings to Wait for TRAP Calls). The Advanced Settings tool is available in Tools Depot.
- Dial out to turn message waiting indicators (MWIs) on and off.
- Dial out to deliver outbound AMIS messages (some systems may not have this feature).
- *(Only integrations of Cisco Unified Communications Manager 4.1 and later with Cisco Unity 4.0(5) and later)* Enable authentication of the Cisco Unity voice messaging ports.
- *(Only integrations of Cisco Unified Communications Manager 4.1 and later with Cisco Unity 4.0(5) and later)* Enable encryption of the media stream.

The number of voice messaging ports set for answering and dialing out depends on many factors, such as:

- The total number of voice messaging ports available.
- The number of subscribers who will use message notification and how often they will receive notifications.
- For circuit-switched phone systems that integrate via voice cards, whether your integration is serial or analog (analog integrations use voice messaging ports to turn MWIs on and off, while serial integrations use an RS-232 serial cable). Circuit-switched phone systems that integrate via PBX-IP Media Gateway units (PIMG units) use voice messaging ports to turn MWIs on and off.
- Whether your organization communicates primarily through e-mail or voice mail.

Each voice messaging port can be set to perform more than one function (for example, to answer calls and to dial out message notifications). When the voice messaging ports perform more than one function and are very active (for example, answering many calls), the other functions may be delayed until the voice messaging port is free (for example, MWIs cannot be turned on until there are fewer calls to answer). For best performance, use the first voice messaging ports only for incoming calls and the last ports only for dialing out. This eliminates the possibility of a collision, in which an incoming call arrives on a port at the same time that Cisco Unity takes the port off-hook to dial out.

In a typical installation, the installer sets up voice messaging ports for Cisco Unity, but you can modify them on the Ports page. Before changing port settings, however, monitor the voice messaging port activity. See the Port Usage Analyzer, available in Tools Depot.

Note If you have a Cisco Unity failover system, voice messaging port settings are not replicated between the primary and secondary servers. You must change voice messaging port settings on both servers.

Remapping Extension Numbers

Remapping Feature Overview

The extension remapping feature lets you convert to the extensions of your choice the calling numbers and forwarding numbers of calls handled by Cisco Unity. This feature is useful, for example, when the phone system cannot map multiple extension numbers on a subscriber phone to a single Inbox.

Remapping can change one or both of the following extension numbers in a call:

- Calling number (the number from which a call originates). For example, Cisco Unity changes the calling number of calls so that the caller ID appears to be a different extension than the one that actually placed the call.
- Forwarding number (the number that a call is going to). For example, unanswered calls to all line extensions on a single phone can be forwarded to the Inbox of a single subscriber; or unanswered calls to phones not assigned to subscribers can be forwarded to the Inbox of a supervisor.

Setting Up Cisco Unity to Remap Extension Numbers

This section includes a procedure for enabling the remapping feature. You can create multiple files in either or both of two directories:

- In the Calling directory, one or more .exm files remap caller ID numbers.
- In the Forwarding directory, one or more .exm files remap numbers that Cisco Unity provides with calls it forwards.

When you create remapping instructions in a .exm file in a directory, Cisco Unity remaps only the type of extension number that the directory is named for. For example, if you want to remap only the extensions that Cisco Unity provides with calls it forwards, you enter the instructions in a .exm file in the Forwarding directory; in this circumstance, the Calling directory needs no .exm file.

In each directory, you can have several .exm files with different file names but with the same .exm extension. This helps you to organize the remapping information. For example, you could create two files in a directory: Ports_1-12.exm and Ports_13-24.exm. Cisco Unity reads all files that have the .exm extension in these directories.

To Remap Extension Numbers

Step 1 On the Cisco Unity server, browse to the **CommServer\IntLib\ExtensionMapping** directory. In this directory is the file Sample.txt and two more directories: Calling and Forwarding.

Step 2 To remap calling numbers, go to the **Calling** directory.

Step 3 In a text editor application, create a new .exm file, or open a currently existing .exm file.

For an example, open the file Sample.txt in the CommServer\IntLib\ExtensionMapping directory.

Caution When opening an .exm file in a text editor, do not associate the file with the text editor by checking the Always Use This Program to Open check box in the Open With dialog box. Otherwise, the .exm file will be saved as a .txt file and the remapping feature will ignore the file.

Step 4 Enter **[Range]** and press **Return** to create a section for indicating which voice messaging ports will be monitored for remapping calls.

A .exm file can have only one [Range] section.

Step 5 Enter **ports=** followed by the numbers of the voice messaging ports, separated by commas. Ranges are designated by a hyphen (-) without spaces. To monitor all voice messaging ports, enter ports=* on this line. Then press **Return**.

For example, you might enter:

ports=1,2,5-34

Step 6 To create a section for the remapping rules, press **Return**, enter **[Number Mappings]**, and then press **Return**.

A .exm file can have only one [Number Mappings] section.

Step 7 Enter one remapping rule on the line, and then press **Return**.

See the remapping rule examples in the following "Syntax and Examples" section. The rule format is:

<original number>, <new number>

The rules cannot include spaces between digits. However, the numbers must be separated by a comma and a single space. Wildcard characters cannot appear at the beginning of a number.

Step 8 For all remaining rules, repeat Step 7.

Step 9 Save and close the .exm file.

Step 10 To remap forwarding numbers, browse to the directory **CommServer\IntLib\ExtensionMapping\Forwarding**.

Step 11 Repeat Step 3 through Step 9 to remap forwarding numbers.

Step 12 For extension remapping to take effect, restart the Cisco Unity software.

Syntax and Examples

Table 11-1 shows the wildcard characters you can use in the .exm files.

Table 11-1 Wildcard Characters

Wildcard	Result
*	Matches zero or more digits.
?	Matches exactly one digit. Use ? as a placeholder for a single digit.

Table 11-2 gives examples for the syntax and results of rules in the .exm files.

Table 11-2 Syntax Examples

Rule	Original Number	New Number
2189, 1189	2189	1189
3189, 1189	3189	1189
4189, 1189	4189	1189

Table 11-2 Syntax Examples (continued)

Rule	Original Number	New Number
2???, 1???	2189	1189
	2291	1291
3???, 1???	3189	1189
	3291	1291
8???, 61???	8000	61000
	8765	61765
123*, 44*	12300	4400
	12385	4485

Cisco Unity executes rules in the order they appear in the .exm file. For example, the .exm file might contain the following rules:

1234, 1189
3189, 1189
4189, 1189
123?, 8891

The extension 1234 would be remapped to 1189 while extensions 1233 and 1235 would be remapped to 8891, because the rule mapping 1234 appears earlier.

An .exm file might contain the following:

[Range]
ports=1,2,5-34

[Number Mappings]
2189, 1189
3189, 1189
4189, 1189
8???, 9???

Working With Cisco Unity Music on Hold

When Music on Hold is enabled, what callers on hold hear depends on the phone system.

Cisco Unified Communications Manager	The first caller on hold in the call holding queue hears a series of holding tones approximately every five seconds. Subsequent callers in the queue for the same extension will hear music on hold that is generated by Cisco Unity system prompts.

Cisco SIP Proxy Server	All callers on hold in the call holding queue hear silence.
Circuit-switched phone systems	The first caller on hold in the call holding queue hears hold music generated by the phone system, if it is configured to provide music on hold. Otherwise, the first caller hears a series of holding tones approximately every five seconds. Even when the phone system is configured to provide music on hold, subsequent callers in the queue for the same extension will hear music on hold that is generated by Cisco Unity system prompts.

The default wait time in the holding queue for the second and subsequent callers is approximately 30 seconds, and is based on the playing time of the music on hold system prompt WAV files. Cisco Unity plays each of the music on hold files in sequence, beginning with the file PHHoldMusic009.wav. If the caller presses 1 to continue to hold, Cisco Unity loops back to the first file, PHHoldMusic000.wav, then plays the next sequentially-numbered file if the caller wants to continue to hold, and so on.

To increase the holding queue wait time for the second and subsequent callers in the call holding queue, re-record the following ten prompts: PHHoldMusic000.wav through PHHoldMusic009.wav, located in the \CommServer\Localize\Prompts\<Language>\<Codec>\AvPHGreet directory. You can use the same music source for each of the prompts, or choose different music for each prompt. If you do not have an automatic call distribution or other call center product installed, you can record custom messages at the beginning or at the end of the music for several of the prompts, for example, “Your call is important to us. We apologize for the delay. A representative will be with you shortly,” or a brief message advertising your products. The playing time for each of these WAV files should be approximately the same, and be from 45 to 120 seconds in length. Be sure to record and test all ten prompts. If any of the ten PHHoldMusic WAV files are missing, callers will hear the fail-safe conversation and be unable to continue holding.

Be aware that subsequent callers in the holding queue cannot advance while a particular WAV file is playing; Cisco Unity takes action on the call at the end of the playing of each WAV file. Therefore, we recommend that you keep the playing time for each of the prompts to the minimum amount of time that meets the needs of your site. (Note, however, that the first caller on hold will be transferred to the extension at whatever point it becomes available.)

Caution Customized system prompt WAV files are not preserved during a Cisco Unity upgrade, or on a system restoration when the backup was made by using the Cisco Unity Disaster Recovery Tools. Keep a copy of your customized music on hold prompt files, so that you can replace the standard music on hold prompts, if applicable, after an upgrade or system restoration.

To set up the recording and playback devices that subscribers will use, see the “Setting Up the Media Master” section on page 28-10. For a complete list of settings that subscribers can change by phone or by using the Cisco Unity Assistant—including call transfer, message notification, and private list settings, see the “Subscriber Orientation” section on page 29-1.

CHAPTER 12

Managing Phone View Features and Remote Message Monitor

See the following sections in this chapter:

Phone View Features

Revised September 29, 2008

Phone View features—such as Message Monitor and Visual Message Locator—use the LCD screens of Cisco IP phones to display information and messages.

Phone View features work only with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) phone systems, and only with supported Cisco IP phones. For details on requirements, see the "Requirements for Cisco Unity Phone View" section in the applicable *System Requirements for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

To set up Phone View features, you first create an application CTI user in Cisco Unified CM and associate the applicable subscriber devices with this user. Then, you enable Phone View features for the phone system. Additionally, Visual Message Locator must be enabled for individual subscribers. Note that subscribers can also change their personal settings to enable Message Monitor for a specified phone, or to disable it.

Do the following procedures in order, as applicable.

To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 5.x and Later)

Step 1 In Cisco Unified Communications Manager Administration, click **User Management > Application User**.

Step 2 On the Find and List Application Users page, click **Add New**.

Step 3 On the Application User Configuration page, do the following sub-steps to create a CTI user account that will have access to all subscriber phones for Phone View:

a. In the User ID field, enter a unique name for the CTI user. For example, enter "PhoneViewUser."

b. In the password field, enter a password for the user.

c. In the Confirm Password field, re-enter the password that you entered in Step 3b.

Step 4 In the credential policy for the Phone View CTI user, ensure that the User Must Change at Next Login and the Does Not Expire check boxes are both unchecked. Otherwise, Phone View will not work.

Step 5 Associate the subscriber phone devices for which you want to enable Phone View with the new CTI user.

Step 6 Click **Save**.

Step 7 Continue with the "To Enable Phone View on the Cisco Unity Server" procedure on page 12-2.

To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 4.x)

Step 1 In Cisco Unified Communications Manager Administration, click **User > Add a New User**.

Step 2 On the User Configuration page, do the following sub-steps to create a CTI user account that will have access to all subscriber phones for Phone View:

a. In the First Name field, enter a first name for the CTI user. For example, enter "PhoneView."

b. In the Last Name field, enter a last name for the CTI user. For example, enter "User."

c. In the User ID field, enter a unique user name. For example, enter "PhoneViewUser."

d. In the password field, enter the password for the user.

e. In the Confirm Password field, re-enter the password that you entered in Step 2d.

f. In the PIN field, enter the PIN for the user.

g. In the Confirm PIN field, re-enter the PIN that you entered in Step 2f.

h. Check the **Enable CTI Application Use** check box.

i. Check the **Enable CTI Super Provider Use** check box.

j. Click **Insert**.

Step 3 Under Application Profiles of CTI, click **Device Association**.

Step 4 On the Device Association page, add the subscriber phone devices for which you want to enable Phone View.

Step 5 Click **Update**.

Step 6 Continue with the following "To Enable Phone View on the Cisco Unity Server" procedure.

To Enable Phone View on the Cisco Unity Server

Step 1 On the Cisco Unity server, on the Windows Start menu, go to **Programs > Unity > Manage Integrations**.

Step 2 In the Manage Integrations utility, click **Properties** for the Cisco Unified Communications Manager phone system to enable for Phone View.

Step 3 Click the **Phone View** tab.

Step 4 In the Phone System Version field, click the version of the Cisco Unified Communications Manager phone system.

Step 5 In the CTI Refresh Interval field, enter the refresh interval in minutes. The default is 15 minutes.

Step 6 Under CUCM/CCM Access, in the User Name field, enter the name of a user with access permission to Cisco Unified CM Administration.

Step 7 In the Password field, enter the password for the user specified in Step 6.

Step 8 Under CTI Phone Access, in the User Name field, enter the name of the CTI Application User that you created to access subscriber phones for Phone View.

Step 9 In the Password field, enter the password for the user specified in Step 8.

Step 10 To enable Message Monitor, check the **Message Monitor Enabled** check box.

Step 11 To enable Visual Message Locator, check the **Visual Message Locator Enabled** check box.

Step 12 Click **Save**.

Step 13 When prompted to restart the Cisco Unity services, click **Yes**.

Step 14 Wait for the services to be stopped and restarted.

Step 15 If you are configuring Visual Message Locator, continue with the following procedure as applicable.

To enable Visual Message Locator for subscribers, you can use either the Cisco Unity Administrator or Bulk Edit.

To enable the feature for a group of existing subscribers at once by using the Bulk Edit utility, do the "To Enable Visual Message Locator by Using the Bulk Edit Utility" procedure on page 12-3.

To enable the feature for an individual subscriber, do the "To Enable Visual Message Locator by Using the Cisco Unity Administrator" procedure on page 12-4.

To Enable Visual Message Locator by Using the Bulk Edit Utility

---

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the Tools Depot window, expand **Administration Tools**, then double-click **Bulk Edit**.

Step 3 In the Unity Bulk Edit Utility window, on the Overview page, click **Next**.

Step 4 On the Select Subscriber page, under Select Subscriber, select the subscribers that you want and click **Add Subscribers to Grid**.

Step 5 Click **Next**.

Step 6 On the Select Subscriber Changes page, click the **Features** tab.

Step 7 Under Finding Messages by Phone, in the Subscribers Can Use Message Locator field, click **True**.

Step 8 In the Include Receipts in Searches field, click **True**.

Step 9 In the Enable Phone View Message Locator Feature field, click **True**.

Step 10 Click **Next**.

Step 11 On the Apply Changes page, click **Update Subscribers**.

Step 12 When you are prompted that the Bulk Edit utility is done, click **OK**.

Step 13 When you are prompted to view the output log, click the applicable button.

Step 14 In the Unity Bulk Edit Utility window, click **Exit**.

To Enable Visual Message Locator by Using the Cisco Unity Administrator

Note You can create a subscriber template in which you enable Visual Message Locator. This will enable the feature for all subsequent subscriber accounts that are created by using the template. Modifying a template to enable the feature does not change settings for existing subscriber accounts.

Step 1 In the Cisco Unity Administrator, find the subscriber for which you are enabling Visual Message Locator.

Step 2 Click **Features**.

Step 3 Check the **Subscriber Can Use Message Locator** check box.

Step 4 Check the **Subscriber Can Use Phone View Visual Message Locator** check box.

Step 5 Check the **Include Receipts in Searches** check box, if applicable.

Step 6 Click **Save**.

Remote Message Monitor

The Remote Message Monitor feature allows voicemail subscribers to listen to a message on a remote phone as the caller records it and gives them the option of connecting to the caller.

To enable the feature, you must first enable it for all subscribers who are associated with a Cisco Unified Communications Manager phone system. Then, subscribers must set up notification for their remote phone by using the Cisco Unity Assistant.

Do the following procedure to enable the feature for all subscribers who are associated with a Cisco Unified CM phone system.

To Enable Remote Message Monitor on the Cisco Unity Server

Step 1 On the Cisco Unity server, on the Windows Start menu, go to **Programs > Cisco Unity > Manage Integrations**.

Step 2 In the Manage Integrations utility, go to the Properties of the Cisco Unified CM integration being enabled for the Remote Message Monitor.

Step 3 Click on the **Phone View** tab.

Step 4 Check the **Remote Message Monitor Enabled** check box.

Step 5 Click **Save**.

Step 6 When prompted to restart the Cisco Unity services, click **Yes**.

Step 7 Wait for the services to be stopped and restarted.

CHAPTER 13

Managing Network Settings

See the following sections in this chapter:

Network Settings Overview

You use network settings to set up and administer Cisco Unity for networking with other Cisco Unity servers and other voice messaging systems. The term networking has a broad definition and encompasses the following ideas:

- Subscribers associated with one Cisco Unity server can use the phone to send voice messages to:
  - Subscribers associated with another Cisco Unity server.
  - Individuals who use a voice messaging system other than Cisco Unity.
  - Individuals with access to a computer connected to the Internet.
- Unidentified callers can find any subscriber in the phone directory and leave a voice message. Depending on the phone system and network configuration, unidentified callers who reach the Cisco Unity automated attendant or directory assistance can be transferred to any subscriber phone, even to the phone of a subscriber who is not associated with the local server.

Cisco Unity provides the following networking options:

- **Digital Networking**—Allows messaging among multiple Cisco Unity servers connected to a single, global directory. The message transport agent (MTA) is the message transport mechanism between servers. You use this option when the Cisco Unity servers access a shared voice mail directory.
- **Internet Subscribers**—Allows messaging between Cisco Unity subscribers and individuals with access to a computer connected to the Internet.
- **AMIS Networking**—Allows messaging between Cisco Unity and other voice messaging systems that support the AMIS protocol.
- **Bridge Networking**—Allows messaging between a Cisco Unity system and an Octel system on an Octel analog network by using the Cisco Unity Bridge.
- **VPIM Networking**—Allows messaging between Cisco Unity and other voice messaging systems that support the VPIM protocol.

No matter which networking option you use, you always customize the primary location settings for your Cisco Unity server. When setting up Cisco Unity to communicate with another voice messaging system, you also need to create a delivery location on your local Cisco Unity server that corresponds to the other voice messaging system.

For more information about networking, see the *Networking Guide for Cisco Unity*. For more information about Bridge Networking, see the *Networking Guide for Cisco Unity Bridge*. Both guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Managing Dialing Domain Options

The dialing domain options allow you to enable the following features for networked Cisco Unity servers that belong to the same dialing domain:

- Cross-server log on *(not available for phone system integrations through voice cards)*. Cross-server log on allows you to provide subscribers with one number that they can call to log on to Cisco Unity from outside the organization. Subscribers call the pilot number for one Cisco Unity server and are transferred to the applicable home Cisco Unity server to log on.

  Note that the intended use of this feature is limited to subscribers calling in from outside your organization, and that:

  - Subscriber phones must still forward calls to the Cisco Unity server that is home to the subscriber.
  - When calling from their extensions, subscribers should still dial the number of their home Cisco Unity server. If subscriber phones have a “Messages” or a speed-dial button that dials the number to access Cisco Unity, the buttons must still be configured to call the Cisco Unity server that is home to the subscriber.
- The transfer method for calls transferred from the automated attendant and directory handlers to Cisco Unity subscribers on other Cisco Unity servers. You choose one of the following transfer methods:
  - Release Calls to the Phone System
  - Cross-Server Transfer *(not available for phone system integrations through voice cards)*
- The transfer method for live reply calls to Cisco Unity subscribers on other Cisco Unity servers. This allows subscribers to reply to messages from Cisco Unity subscribers on another Cisco Unity server by calling them. Note that whether subscribers have access to the live reply feature is controlled by the class of service message settings. You choose one of the following transfer methods for the live reply call:
  - Release Calls to the Phone System
  - Cross-Server Live Reply *(not available for phone system integrations through voice cards)*

Determining AMIS Schedules

The AMIS schedule and the AMIS restriction table together determine when outgoing AMIS calls are made. If a delivery number for an outgoing AMIS message is allowed by the AMIS restriction table, the message is sent immediately—the schedule settings do not apply. If the delivery number is not allowed

by the AMIS restriction table, the schedule determines when the message is sent. Therefore, the schedule determines when messages are sent for delivery numbers that are disallowed by the AMIS restriction table.

Cisco Unity batches messages to a delivery location, with a maximum of nine messages per batch. If an AMIS transmission is in progress when the schedule becomes inactive, the transmission of the entire batch of messages is completed. However, any other messages remaining in the queue, but not in the batch that was in the process of being transmitted, are queued until the next active time in the schedule. Queued messages are placed in the UAmis mailbox.

Because the transmission of AMIS messages may tie up voice ports for long periods of time, you may want to schedule outgoing AMIS calls during closed hours or at times when Cisco Unity is not processing many calls. Additionally, if most or all of your AMIS delivery numbers are long distance, you may want to schedule the AMIS calls when the long distance phone rates are lower.

CHAPTER 14

Cisco Unity Conversation Overview

When callers access Cisco Unity by phone, they hear a set of prerecorded instructions and options known as the Cisco Unity conversation—or the TUI (telephone user interface). Unidentified callers hear the unidentified caller conversation, which enables them to access the Cisco Unity automated attendant, conduct subscriber searches by using directory assistance, use call routing options, and play audiotext messages. Subscribers hear the subscriber conversation, which enables them to log on to Cisco Unity, enroll as new subscribers, send and receive messages, record greetings, and change their personal settings.

See the following sections in this chapter:

Summary of How You Can Customize Cisco Unity Conversations

You can customize the conversations that subscribers and unidentified callers hear in several ways.

- **Broadcast messages**—Specify that subscribers can use Cisco Unity to do the following tasks:
  - Send broadcast messages to other subscribers on same server.
  - Send broadcast messages to subscribers on multiple servers.
  - Update previously recorded broadcast messages that are stored on local server.

  Default: Disabled.

  Scope: Individual subscribers and/or groups.
- **Call handlers**—You can customize the predefined call handlers or create your own. You may want to use a call handler in the following ways:
  - As an automated attendant.
  - To offer prerecorded audiotext.
  - As a message recipient.
  - To transfer calls.

  Scope: All subscribers and/or outside callers per server.
- **Call holding wait time and music**—You can configure call waiting hold time. You can also customize the music that callers hear while on hold.

Scope: All subscribers and/or outside callers per server.

- **Call routing**—You can customize how Cisco Unity handles direct calls and forwarded calls.

  Based on criteria such as the phone number of the caller and the schedule that you specify, you can route certain calls to the Operator call handler, Opening Greeting, a subscriber greeting, the subscriber logon conversation, and so on.

  Scope: All subscribers and/or outside callers per server.

- **Caller ID**—You can enable Cisco Unity to provide subscribers with additional information about callers who leave messages for them.

  Scope: Individual subscribers and/or groups.

- **Caller input**—For subscriber greetings, you can define the actions that Cisco Unity takes in response to touchtone keys pressed by callers.

  Default: Enabled with the *, 0, or # keys mapped as follows:

  - The * key is set up to offer the Sign-In conversation.
  - The # key is set up to skip greetings.
  - The 0 key is set up to send callers to the Operator call handler.

  Scope: Individual subscribers and/or groups.

- **Deleting messages**:

  You can:

  - Dictate whether subscribers can listen to, reply to, or forward deleted messages, or restore them as new or saved messages (this setting applies at the class of service (COS) level).
  - Change how Cisco Unity handles the way in which multiple deleted messages are deleted.
  - Enable Cisco Unity to request confirmation from subscribers before proceeding with a deletion of a single deleted message. (To delete a deleted message, subscribers must belong to a class of service that allows them to retain and review deleted messages.) Default: Disabled.
  - Enable Cisco Unity to request confirmation from subscribers before proceeding with a deletion of a single new or saved message. Default: Disabled.

  Note that the Cisco Unity conversation plays the menu that offers the deleted messages option to all subscribers—even those who do not have COS rights to access deleted messages. You can specify that Cisco Unity plays the menu offering access to deleted messages only to subscribers who have COS rights to access them.

  Scope: All subscribers per server.

  To change whether the Cisco Unity plays the menu that offers the deleted messages option, see Advanced Settings tool Help (in the Unity Settings list, click Conversation—Do Not Offer Deleted Messages Option). The Advanced Settings tool is available in Tools Depot.

- **Directory handlers**—You can specify:

  - Search scope.
  - Whether a directory handler searches for subscribers first name first, or last name first.
  - What subscribers and callers hear when the directory handler finds one or more matches.
  - What the directory handler does when it detects no caller input.

  You can also set up multiple directory handlers to provide directory searches for systems with hundreds or thousands of subscribers.

  Scope: All subscribers and/or outside callers per server.

- **Finding messages**—You can enable subscribers to use Message Locator to find voice messages—or voice messages, receipts, and notices—from Cisco Unity subscribers and outside callers when they check messages by phone.

  Default: Disabled.

  Scope: Individual subscribers and/or groups.

- **First-time enrollment**—You can specify that when subscribers log on for the first time (or the next time, as applicable), Cisco Unity prompts them to enroll. The first-time enrollment conversation asks subscribers to record a name and greeting, set a password, and choose whether to be listed in directory assistance.

  Note that Cisco Unity does not prevent subscribers from completing the enrollment process if they do not record their names. You can change the first-time enrollment conversation so that it requires subscribers to record a voice name to complete first-time enrollment.

  Default: First-time enrollment is enabled, but subscribers are not required to record a voice name.

  Scope: Individual subscribers and/or groups; all subscribers per server (require recorded name).

  To require all subscribers to record a voice name during enrollment, see Advanced Settings tool Help (in the Unity Settings list, click Conversation—First-Time Enrollment: Require Subscribers to Record Names). The Advanced Settings tool is available in Tools Depot.

- **Forwarding messages: prompting subscribers to record introductions—**You can indicate if you want Cisco Unity to prompt subscribers to record introductions when they forward messages.

  Note that this setting has no effect on the conversation when Cisco Unity is set to prompt subscribers to record first and then address messages.

  Default: Cisco Unity does not prompt subscribers to record introductions. Subscribers must press 2 to record an introduction.

  Scope: All subscribers per server.

  See Advanced Settings tool Help. The setting is called Conversation**—**Subscriber Forward Message Flow (Prompt for Introduction). The Advanced Settings tool is available in Tools Depot.

- **Full Mailboxes**—You can specify that Cisco Unity checks whether a subscriber mailbox is full when an outside caller tries to leave a message for the subscriber. If the mailbox is full, the outside caller will be told that he or she cannot record a message for the subscriber.

  Default: Disabled.

  Scope: All subscribers and/or outside callers per server.

- **Greetings: alternate greeting notification, enabling notices, and specifying caller options**—Because the alternate greeting overrides all other greetings, subscribers can use the alternate greeting for a variety of special situations, such as vacations, leave of absence, or a holiday. When it is enabled, you can specify that Cisco Unity:
  - Plays a prompt to remind subscribers that their alternate greeting is enabled.
  - 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 when they leave, send, reply to, or forward messages to other subscribers who have their alternate greeting enabled.

  Default: Disabled.

Scope: Individual subscribers and/or groups; enabling alternate greeting notices can only be done per server.

- **Greetings: enabling callers to transfer from subscriber greetings to an alternate contact number**—You can set up Cisco Unity so that callers can transfer to an alternate contact number by pressing a key during the greetings for a particular subscriber or a group of subscribers.

  Scope: Individual subscribers and/or groups.

- **Greetings: maximum length**—You can set the maximum recording length allowed for subscriber greetings.

  Default: 90 seconds.

  Scope: Subscriber groups.

- **Greetings: setting up**—You can enable up to five greetings for each subscriber and call handler. You specify how long each greeting is enabled, the greeting source, and the actions that Cisco Unity takes during and after each greeting.

  Scope: Individual subscribers and/or groups.

- **Identified Subscriber Messaging (ISM)**—ISM affects what subscribers hear when they call other subscribers from their primary or alternate extensions and are forwarded to the greetings of the subscribers they call. If they then leave a message, ISM affects what the called subscriber hears and can do when listening to the message.

  When ISM is enabled, Cisco Unity recognizes that the calling extension is associated with a subscriber and accordingly plays the internal greeting of the called subscriber. Additionally, when the called subscriber later listens to the message, Cisco Unity plays the recorded voice name of the subscriber who left the message and allows the called subscriber to record a reply.

  Default: Enabled.

  Scope: All subscribers and/or outside callers per server.

  For an explanation of how ISM works with remote subscribers, and for information on how to set it up, see the *Networking Guide for Cisco Unity* or the *Networking Guide for Cisco Unity Bridge*, as applicable. Both guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

- **Interview handlers**—You can specify:
  - What questions the interview handler asks.
  - The recipient of the interview response.
  - The extension (if any) that callers dial to reach the interview handler.
  - The language in which callers hear system prompts.

  Scope: All subscribers and/or outside callers per server.

- **Language: settings for routing rules and call handlers**—You can customize the language settings for routing rules, call handlers, interview handlers, and directory handlers.

  Scope: Individual conversation components.

- **Language: settings for specific subscribers**—You can specify which language callers hear when they leave messages for individual subscribers. (This affects prompts such as “Record your message at the tone.”)

  Scope: Individual subscribers and/or groups.

- **Language: system prompts**—You can specify the default language in which system prompts are played to all subscribers and callers.

Scope: All subscribers and/or outside callers per server.

- **Language: Text to Speech (TTS)**—You can specify the default TTS language that subscribers hear when having their e-mail read to them over the phone.

  Scope: Individual subscribers and/or groups.

- **Leaving messages: enabling and customizing a warning tone (Cisco Unified Communications Manager and SIP phone system integrations only)**—You can enable a warning tone to play before the maximum allowable message length of a recording is reached.

  You can also customize the tone by recording a WAV file with another tone or a brief message.

  Default: Disabled.

  Scope: All subscribers and/or outside callers per server.

- **Leaving messages: enabling a "post-greeting recording"**—You can specify whether Cisco Unity plays a recording before allowing callers to leave a message for subscribers assigned to a class of service (COS).

  For each COS, you use the Media Master control bar on the page to record what you want callers to hear, and you indicate whether all callers hear the recording or only unidentified callers. Though callers can press # to skip a subscriber or call handler greeting, callers cannot skip a "post-greeting recording."

  Default: Disabled.

  Scope: Groups of subscribers.

- **Leaving messages: maximum message length for unidentified callers**—You can set the maximum message length allowed to unidentified callers.

  Scope: Individual subscribers and/or groups.

- **Leaving messages: playing the "Record your message at the tone" prompt**—You can indicate if you want Cisco Unity to tell callers to record their message after the tone.

  Default: Cisco Unity plays the "Record your message at the tone" prompt after playing a subscriber or call handler greeting. Because some subscribers instruct callers when to record their messages in their greetings, callers hear the instruction twice. For this reason, you may want to specify that Cisco Unity does not play the prompt after some or all greetings when callers leave messages for particular subscribers or call handlers in your organization.

  Scope: Individual subscribers and/or groups.

- **Leaving messages: what unidentified callers can do**—You can dictate whether the Cisco Unity conversation offers callers the opportunity to edit the messages that they leave for subscribers, and allows them to mark messages urgent.

  Scope: Individual subscribers and/or groups.

- **Live Record**—Live record allows subscribers to record conversations while they talk to callers.

  Default: Disabled.

  Scope: All subscribers per server.

- **Logging off**—You can select the destination—such as a call handler, interview handler, subscriber, or directory assistance—that Cisco Unity sends subscribers to when they exit the subscriber conversation.

  Scope: Individual subscribers and/or groups.

- **Logging on**—For subscribers on each Cisco Unity server, you can 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.
  - What subscribers hear after Cisco Unity prompts them to log on.
  - Whether they need to enter a password to log on when calling from a known extension or device. (By default, subscribers are always required to enter a password.)

  You can also set up cross-server logon for multiple Cisco Unity servers. Cross-server logon allows you to provide subscribers with one phone number that they can call to log on to Cisco Unity from outside your organization.

  Scope: Individual subscribers and/or groups for single or networked servers.

- **Playing messages: disconnected calls**—You can specify that messages are marked saved upon hang-up or disconnection. You can also enable Dropped Call Recovery for calls dropped during message playback.

  Scope: Individual subscribers and/or groups.

- **Playing messages: excluding all receipts**—You can exclude nondelivery receipts (NDRs) and return (read and delivery) receipts from the list of messages that the Cisco Unity conversation plays for subscribers.

  Default: All receipts are included.

  Scope: All subscribers per server.

  See Advanced Settings tool Help. The setting is called Conversation—Exclude All Receipts From Voice Mail Stack. The Advanced Settings tool is available in Tools Depot.

- **Playing messages: excluding return receipts**—You can exclude return receipts (read and delivery) from the list of messages that are played for subscribers.

  Default: Read receipts are included.

  Scope: All subscribers per server.

  See Advanced Settings tool Help. The setting is called Conversation—Exclude Return Receipts From Voice Mail Stack. The Advanced Settings tool is available in Tools Depot.

- **Playing messages: fast-forwarding and rewinding messages**—You can specify the amount of time that Cisco Unity skips back or ahead in a message when subscribers are listening to messages and they rewind or fast-forward the message.

  Default: 5 seconds.

  Scope: Individual subscribers and/or groups.

- **Playing messages: jumping to first or last message**—By using the Custom Key Map utility, you can give subscribers the option to jump to the first or last message in the message stack while they are listening to messages.

  Scope: Individual subscribers and/or groups.

- **Playing messages: message playback options**—You can dictate whether subscribers hear the Message Type menu, message counts, and timestamps when they check messages, and you can specify the order in which Cisco Unity plays messages.

  Scope: Individual subscribers and/or groups.

- **Playing messages: play new messages automatically**—You can specify that Cisco Unity plays new messages after subscribers log on without requiring them to press 1 from the Main menu (“Press 1 for new messages”).

  Default: New messages are not played automatically.

Scope: Individual subscribers and/or groups.

- **Playing messages: prioritizing received messages**—By using the Custom Key Map utility, you can give subscribers the option to toggle the priority of a message from normal to urgent, and vice versa.

  Scope: Individual subscribers and/or groups.

- **Recorded names: maximum recorded name length**—You can specify the number of seconds allowed for subscriber recorded names.

  Scope: Subscriber groups.

- **Recording time limits**—You can specify:
  - How much to truncate the end of a recording when a message is terminated with a touchtone.
  - Silence thresholds before, during, and after recordings.
  - The number of seconds that Cisco Unity uses as a cutoff for short and long recordings.
  - The minimum length of recordings, in seconds, for messages or greetings.

  Scope: All subscribers and/or outside callers per server.

- **Replaying messages**—You can change the Cisco Unity conversation so that it replays only the message body when a subscriber replays a voice message.

  Default: Cisco Unity replays both the summary and the body of the message.

  Scope: All subscribers per server.

  See Advanced Settings tool Help. The setting is called Conversation—Do Not Replay Message Summary. The Advanced Settings tool is available in Tools Depot.

- **Replying to messages: "Live Reply"**—On each Cisco Unity server, you can enable subscribers to reply to messages from other subscribers by calling them.

  You can also enable cross-server live reply to subscribers on networked Cisco Unity servers. Cross-server live reply allows subscribers to "live reply" to messages from subscribers on other Cisco Unity servers in a dialing domain.

  Default: Disabled.

  Scope: Subscriber groups for single or networked servers.

- **Replying to messages: unidentified callers**—You can change the Cisco Unity conversation so that it offers the reply option for messages from unidentified callers. In this way, subscribers can reply to subscribers who leave messages as unidentified callers by pressing the same key that they press when they respond to messages from identified subscribers.

  Default: Cisco Unity does not offer the reply option in the After Message menu when the message is from an unidentified caller.

  Scope: All subscribers per server.

  See Advanced Settings tool Help. The setting is called Conversation—Reply to Unknown Caller. The Advanced Settings tool is available in Tools Depot.

- **Responding to phone menus: timeouts for outside callers and subscribers**—For outside callers and for each subscriber, you can specify the following:
  - How long Cisco Unity waits for the caller or subscriber to press a key after playing a menu.
  - How long Cisco Unity waits for additional key presses after the caller or subscriber has pressed a key when entering subscriber names or extensions to address a message, update passwords, change call transfer or message notification numbers, and the like.

  - How long Cisco Unity waits for additional key presses after the caller or subscriber has pressed a key that represents the first digit of more than one possible key combination in a particular phone menu. (For example, in the After Message menu for the standard conversation, subscribers can press 4 to reply to a message, 42 to reply to all, or 44 to call the subscriber.) This also applies when subscribers use ## to switch addressing modes.
  - How many times Cisco Unity repeats a menu if the caller or subscriber has not responded to a menu.

  Scope: Outside callers per server. Individual subscribers and/or groups.

- **Securing voice messages**—You can set up secure messaging and enable subscribers to use it. Secure messaging provides security through the use of public/private key encryption for voice messages that subscribers record by using the Cisco Unity conversation.

  Voice messages that are marked secure can be played by using the phone interface, Cisco Unity Inbox or Cisco Unity ViewMail for Microsoft Outlook as long as the interfaces can authenticate the subscriber with the Cisco Unity server.

  Default: Disabled.

  Scope: Outside callers per server. Individual subscribers and/or groups.

- **Sending messages: address by name or number**—You can determine how Cisco Unity prompts subscribers to address messages to other subscribers when they send messages ("Press 2 to send a message"): by entering extensions, by spelling first names, or by spelling last names.

  (When spelled name searches are enabled for the server, subscribers can switch between addressing by name and addressing by extension by pressing ## or 00.)

  Scope: Individual subscribers and/or groups.

- **Sending messages: address confirmation**—You can alter how Cisco Unity prompts a subscriber to confirm message addressing when they send messages ("Press 2 to send a message").

  Scope: All subscribers per server.

- **Sending messages: addressing order**—You can change the order in which Cisco Unity prompts subscribers to address and record messages.

  Scope: Individual subscribers and/or groups.

- **Sending messages: disconnected calls**—You can specify whether messages are sent when subscriber hangs up or call is disconnected. You can also enable Dropped Call Recovery for calls dropped while addressing or recording messages.

  Scope: Individual subscribers and/or groups.

- **Sending messages: double-key time interval for addressing**—You can adjust the time that Cisco Unity waits for the second # or 0 key when subscribers switch between addressing by name and ID.

  Consider changing the interval of time that Cisco Unity uses to interpret the two key presses if subscribers complain that Cisco Unity does not act upon key presses as they expect.

  Scope: Individual subscribers and/or groups.

- **Sending messages: maximum message length for subscribers**—You can set the maximum message length allowed to subscribers.

  Default: 300 seconds.

  Scope: Individual subscribers and/or groups.

- **Sending messages: public distribution lists**—You can specify whether subscribers can send messages to public distribution lists.

Scope: Subscriber groups.

- **Sending messages: sending a quick message while listening to messages**—By using the Custom Key Map utility, you can provide subscribers with the option to send "quick messages." After listening to a message, a subscriber can press the applicable key to quickly switch to the send message conversation to send a message; when the message has been sent, the subscriber is then returned to the message playback conversation.

  Scope: Individual subscribers and/or groups.

- **Sending messages: continuous addressing**—You can specify that Cisco Unity allows subscribers to continue adding names after adding a recipient. In this way, you can significantly streamline the addressing process when subscribers send and forward messages to multiple recipients.

  Scope: All subscribers per server.

- **Skipping messages (Optional conversation 1 only)**—You can specify whether Cisco Unity saves new messages that subscribers have skipped by pressing # during message playback: as saved messages or as new messages.

  Default: Saved as new.

  Scope: All subscribers per server.

- **Skipping messages (standard conversation only)**—You can specify whether Cisco Unity fast-forwards to the end of a message or skips to the next message when subscribers press the # key during message playback.

  Default: Cisco Unity fast-forwards to the end of the message and then plays the After Message menu. Subscribers press ## to skip to the next message during message playback.

  Scope: All subscribers per server.

- **Speed control: prompts for subscriber conversation**—You can specify the speed at which Cisco Unity plays prompts—including recorded voice names, receipts, message headers and footers, and subscriber greetings—to subscribers.

  Scope: Individual subscribers and/or groups.

- **Speed control: subscriber messages**—You can specify how fast Cisco Unity plays the body of subscriber messages and recorded introductions for fax messages when subscribers play their messages over the phone.

  Note that the speed that you specify for message playback does not affect the speed of Text to Speech (TTS) messages, receipts, or message headers and footers: TTS messages are always played at normal speed, while the speed at which Cisco Unity plays receipts, message headers, and message footers are determined by the prompt speed specified for the Cisco Unity conversation.

  Subscribers can use the Media Master control bar to adjust speed of messages that they play by using computer speakers.

  Scope: Individual subscribers and/or groups.

- **Spelled name searches and addressing**—You can specify whether Cisco Unity allows subscribers to search for and address messages to other subscribers by spelling names.

  Default: Enabled.

  Scope: All subscribers per server.

- **Style of all phone menus**—You can specify that subscribers hear the comprehensive instructions offered by the full menus, or that they hear brief menus.

  Default: Full.

  Scope: Individual subscribers and/or groups.

- **Style of Main menus**—You can specify the keys mapped for the Main menu options by using the Custom Keypad Mapping utility and assigning subscribers to a custom conversation style.

  Scope: Individual subscribers and/or groups.

- **Style of message-retrieval menus**—You can select the conversation style that subscribers hear when they play their messages over the phone. Each style offers a different keypad mapping for the message-retrieval menus, and one even allows you to specify your own keypad mapping. You can also select which conversation styles subscribers can select for themselves by using Cisco Unity Assistant.

  Other menus—those that unidentified callers and Cisco Unity subscribers use to change their Cisco Unity settings—are the same for each conversation style.

  Default: Standard.

  Scope: Individual subscribers and/or groups.

- **Style of send menus**—You can select the style of menus that subscribers hear when they send, reply to, and forward messages over the phone: standard or streamlined.

  When you select a send menu style, consider that the streamlined style enables subscribers to use fewer keystrokes to mark messages urgent, request receipts, and perform other tasks. In addition, the streamlined style offers easier navigation of lists when they address messages.

  Default: Streamlined.

  Scope: Individual subscribers and/or groups.

- **Transfer and holding options**—You can dictate some of what subscribers and unidentified callers hear when Cisco Unity transfers a call from the automated attendant or a directory handler to a subscriber, including what they hear when they are on hold.

  For example, depending on how you set up Cisco Unity and the phone system to handle call transfers, you may be able to use call transfer settings to:

  - Select what Cisco Unity says and does when the subscriber phone is busy.
  - Determine what Cisco Unity plays when transferring calls.
  - Set up call screening.

  Scope: Individual subscribers and/or groups.

- **Transfers: across networked servers**—Cross-server transfer allows for transfers of calls from the automated attendant or a directory handler of one Cisco Unity server to a subscriber on another Cisco Unity server in the dialing domain.

  Scope: All subscribers and/or callers for networked servers.

- **Transfers: enabling callers to transfer from subscriber greetings to an alternate contact number**—You can set up Cisco Unity so that callers can transfer to an alternate contact number by pressing a key during the greetings for a particular subscriber or a group of subscribers.

  Scope: Individual subscribers and/or groups.

- **Transfers: offering "system transfers"**—You can set up call handler greetings, subscriber greetings, and/or routing rules to allow subscribers to dial internal phone numbers that are not associated with Cisco Unity subscribers.

  By default, Cisco Unity prompts subscribers and callers to confirm the number that they enter before performing the transfer. You can disable the prompt.

  Scope: Individual subscribers and/or groups.

- **Transfers: playing the "Wait while I transfer your call" prompt**—You can indicate whether Cisco Unity notifies callers when it transfers a call.

  Default: Cisco Unity plays the "Wait while I transfer your call" prompt when it transfers a call to an extension. Some callers do not like hearing the prompt, and for this reason, you may want to specify that Cisco Unity does not play it.

  Scope: All subscribers and/or outside callers per server.

- **Transfers: restricting phone numbers**—You can specify which phone numbers subscribers can use for transferring calls.

  Scope: Subscriber groups.

- **TTY**—You can install TTY prompts so that subscribers and unidentified callers who use TTY can call Cisco Unity and use the same features that a hearing caller can use, with a few exceptions.

  Scope: Individual subscribers and/or groups.

- **Volume: message playback (for integrations via phone cards only)**—You can select the volume level at which Cisco Unity plays the body of subscriber messages and recorded introductions for fax messages when subscribers play their messages over the phone.

  Note that the volume that you specify for message playback does not affect the volume of Text to Speech (TTS) messages, receipts, or message headers and footers.

  Subscribers can use the Media Master control bar to adjust volume of messages that they play by using computer speakers.

  Scope: Individual subscribers and/or groups.

- **Volume: system prompts**—You can select the volume level at which all callers hear Cisco Unity system prompts.

  Scope: All subscribers and/or outside callers per server.

  See the Set Volume utility Help. The Set Volume utility is an Audio Management tool, available in Tools Depot.

Summary of How Subscribers Can Customize the Cisco Unity Conversation

Subscribers can customize the Cisco Unity conversation by phone or by using the Cisco Unity Assistant. Table 14-1 details the conversation settings that subscribers can change.

Table 14-1 Settings That Subscribers Can Change

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Call Holding and Screening[1]: • Select how Cisco Unity handles indirect calls when the subscriber phone is busy, including placing the caller on hold, prompting the caller to hold or leave a message, and sending the caller directly to the greeting • Select how Cisco Unity handles indirect calls, including telling the subscriber who the call is for, announcing that Cisco Unity is transferring the call, prompting the subscriber to accept or refuse a call, and prompting callers to say their names	Call Holding and Screening[1]: • None
Call Transfers[2]: • Transfer indirect calls to an extension or send to the greeting • Enable or disable transfer rules • Change extension	Call Transfers[2]: • Transfer indirect calls to an extension or send to the greeting • Enable or disable transfer rules • Change extension
Caller Options: • Allow callers to edit messages • Allow callers to mark messages urgent	Caller Options: • None
Phone Menu Options: • Set language for Cisco Unity prompts • Select full or brief Cisco Unity conversation menus • Specify the conversation style • Enable or disable the Press-or-Say phone input style • Select the action that Cisco Unity performs when the subscriber calls Cisco Unity, including greeting the subscriber by name, playing messages automatically and announcing the number of new messages by type • Change the speed of prompts, recorded names, and subscriber greetings • Configure timeout settings that apply when responding to phone menus	Phone Menu Options: • Select full or brief Cisco Unity conversation menus • Enable or disable the Press-or-Say phone input style
Greetings: • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting • Switch between system prompt and personal greeting • Specify whether callers hear “Record your message at the tone” prompt after greeting	Greetings: • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting

Table 14-1 Settings That Subscribers Can Change (continued)

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Message Notification: • Enable or disable a notification device, and change its number • Specify dialing options • Select the types of messages and message urgency for which Cisco Unity will call a device • Set up a notification schedule, and specify what happens when a device does not answer, is busy, or fails	Message Notification: • Enable or disable a notification device, and change its number
Message Playback: • Specify message playback order • Change the time format used for message time stamps • Select the action that Cisco Unity performs when messages are played, including announcing the name and number of the sender who left a message, whether the timestamp is played before or after the message • Specify whether Cisco Unity plays the Message Type menu • Change the speed and volume of messages that are played over the phone[3] • Specify the amount of time to skip back or ahead when rewinding or fast-forwarding messages • Specify whether Cisco Unity will ask to confirm deletions of new and saved messages • Specify that messages are marked saved upon hang-up or disconnection • Specify that receipts are included in Message Locator searches • Enable Dropped Call Recovery for calls dropped during message playback	Message Playback: • Speed and volume of message as it is played[3]

Table 14-1 Settings That Subscribers Can Change (continued)

Settings That Can Be Changed by Using the Cisco Unity Assistant	Settings That Can Be Changed by Using the Phone Menus
Message Addressing and Sending: • Specify Send Menu Style • Specifying the addressing and recording order • Switch between addressing messages to other subscribers by name, or by extension • Specify order for addressing messages by name (last name followed by first name, or vice versa) • Specify that Cisco Unity prompt to confirm addressee by name • Specify that Cisco Unity continue adding names after each addressee • Specify that Cisco Unity send message when subscriber hangs up or call is disconnected • Enable Dropped Call Recovery for calls dropped while addressing or recording messages	Message Addressing and Sending: • Switch between addressing to other subscribers by name or by extension (by pressing ## or 00)[4]
Personal Settings: • Record a name • Specify a fax delivery number • Change directory listing status • Change password • Specify alternative extensions or devices • Specify an alternate contact number	Personal Settings: • Record a name • Specify fax delivery number • Change directory listing status • Change password • Specify an alternate contact number
Private Lists: • Enter a display name • Record a list name • Add and delete members	Private Lists: • Record a list name • Add and delete members

1. Call holding and screening options apply only to incoming calls that were routed to the subscriber from the automated attendant or a directory handler, and not on direct calls. Holding and screening options do not apply when an outside caller or another subscriber dials a subscriber extension directly. In addition, holding and screening options are only available when supervised transfers are enabled.
2. Call transfer options apply only to incoming calls that were routed to the subscriber from the automated attendant or a directory handler, and not on direct calls. Transfer options do not apply when an outside caller or another subscriber dials a subscriber extension directly.
3. Volume works for integrations via phone cards only. Also, the speed and volume that you specify for messages does not affect Text to Speech (TTS) messages, receipts, or message headers and footers.
4. Note that this depends on whether you have enabled spelled name addressing.

Using the Custom Keypad Mapping Utility to Customize the Conversation

You can use the Custom Keypad Map utility to specify the keypad mapping that subscribers hear when they access Cisco Unity by phone. The utility allows you to map keys for the Main menu and the message-retrieval menus. You can also use the utility to add and remove menu options and to generate a wallet-sized user card PDF file, which you can give to subscribers.

There are several custom mapping styles available for use. The Custom Key Map utility allows you to reset a Custom Keypad Mapping conversation to the keys used for the standard, Optional 1, Alternate Keypad Mapping N, Alternate Keypad Mapping S, or Alternate Keypad Mapping X conversation. This can be useful when you want to make only a few changes to a conversation. (The Custom Keypad Mapping conversations are based on the standard conversation as a starting point.) You can also reset a Custom Keypad Mapping conversation to the keys that Cisco uses in our internal deployment.

To enable subscribers to hear your customized conversation style, specify one of the Custom Keypad Mapping as the conversation style on the Conversations pages for subscriber templates and for individual subscribers in the Cisco Unity Administrator. Alternatively, you can use the Bulk Edit utility to change the conversation style for multiple subscribers at once. Subscribers can also select the conversation style themselves on the Phone Menu Preferences page in the Cisco Unity Assistant.

Note The Wallet Card wizard is available for producing a PDF file of a wallet card based on your custom keypad mappings and that can be printed for distributing to subscribers. For more details, see the "Subscriber Orientation" section on page 29-1.

See the following sections for details on features that are only available when using a Custom Keypad Mapping conversation:

- Offering Subscribers a "Quick Message" Option, page 14-15
- Offering Subscribers the Option to Change the Priority of Messages by Marking Them Urgent or Normal, page 14-16
- Offering Subscribers the Option to Jump to the First or Last Message in a Stack, page 14-16
- Customizing the Subscriber Setup Options Menu, page 14-16
- Offering More Options at the Main Menu, page 14-17
- Offering the Option to Revert to Default Message Playback Speed, page 14-17

The Custom Keypad Map utility is available in Tools Depot. To learn how to use it, see Custom Keypad Map Help.

Offering Subscribers a "Quick Message" Option

By using the Custom Key Map utility, you can provide subscribers with the option to send "quick messages." After listening to a message, a subscriber can press the applicable key to quickly switch to the send message conversation to send a message; when the message has been sent, the subscriber is then returned to the message playback conversation, to the exact spot in the message stack he or she was in before sending the quick message. When the subscriber presses the quick message key, the conversation announces "sending quick message"; when the message has been sent, the conversation then announces "returning to message" as an audible cue to the subscriber.

This functionality is only available while the After Message menu plays.

Note the following behaviors:

- When subscribers send quick messages, they will hear the same send menu style that they normally hear, and the recording and addressing order will be the same.
- Subscribers will only be allowed to send a single quick message before being returned to the message playback conversation. If the subscriber wants to send additional quick messages, the applicable quick message key must be pressed again.

Offering Subscribers the Option to Change the Priority of Messages by Marking Them Urgent or Normal

By using the Custom Key Map utility, you can give subscribers the option to toggle the priority of a message from normal to urgent, and vice versa. Subscribers can toggle the message priority during message playback, and also as the After Message menu plays. When the subscriber presses the applicable key, the priority of the current message is toggled: if the message is currently marked urgent, then it will be set to normal priority; if the message is currently marked normal, then it will be set to urgent priority. The conversation announces the new priority setting for the message, and then moves on to the next message in the stack.

Note the following behaviors:

- When a subscriber toggles the priority of a message, the “new” or “saved” status of the message does not change.
- If the subscriber presses the applicable key to change the priority of a message while listening to it, the conversation will stop playing the message, announce the new priority setting, and then move to the next message, in effect skipping over the message.
- The order of messages in the subscriber stack will not be updated to reflect the new priority of the toggled message until the subscriber leaves the stack by hanging up, or by backing out to the main menu.

Offering Subscribers the Option to Jump to the First or Last Message in a Stack

By using the Custom Key Map utility, you can give subscribers the option to jump to the first or last message in the message stack while they are listening to messages. This option is available in the new, saved, and deleted message stacks. While listening to messages, the subscriber presses the applicable key. The conversation then jumps to the requested message, announcing either “first message” or “last message” as an audible cue to the subscriber.

This functionality is available during message playback and also while the After Message menu plays.

Customizing the Subscriber Setup Options Menu

By using the Custom Key Map utility, you can specify whether the following options are offered to subscribers as part of the Setup Options menu:

- Greetings
- Message Settings
  - Message Notification
  - Fax Delivery

  - Menu Style
  - Private Lists
- Personal Settings
- Transfer Settings

When the Greetings, Personal Settings, and Transfer Settings menus are specified, all options in those menus are also included. Only the options in the Message Settings menu can be specified individually.

Offering More Options at the Main Menu

By using the Custom Key Map tool, you can specify whether the following options are added to the Main menu:

- Subscriber System Transfer
- Greetings Administrator
- Broadcast Message Administrator

Offering the Option to Revert to Default Message Playback Speed

By using the Custom Key Map tool, you can map a key that when pressed during message playback will revert the message playback speed to the default playback speed for the subscriber. This key can be used by subscribers who have changed the playback speed, but want to go back to their default speed while listening to a message.

CHAPTER 15

Managing System-Wide Conversation Settings

See the following sections in this chapter:

About System Prompts

System prompts are standard recordings that come with the Cisco Unity system. The prompts are played in different combinations in multiple places in the phone conversation. All system prompts are located in the CommServer\Localize\Prompts directory and subdirectories.

You can specify the default language in which system prompts are played to all subscribers and callers. See the "Phone Language Settings" section on page 10-6.

You cannot change what the system prompts say by using the Cisco Unity Administrator, the Cisco Unity Assistant, or the phone conversation. Customizing system prompts is not supported. Do not delete system prompts, as this can cause system errors. All system prompts are automatically deleted and replaced when you upgrade Cisco Unity (including maintenance upgrades).

Changing How Cisco Unity Saves New Messages That Subscribers Skip During Message Playback (Optional Conversation 1)

You can customize Optional Conversation 1 to change how Cisco Unity handles new messages that subscribers skip during message playback. By default, when subscribers press # to skip a new message during message playback, Cisco Unity saves the message as new. This means that when subscribers call Cisco Unity to check messages, the skipped message remains in the list of new messages that Cisco Unity plays. In addition, message waiting indicators (MWI) on subscriber phones remain lit as long as there are new messages.

By using the Advanced Settings Tool to change the registry, you can customize Optional Conversation 1 so that Cisco Unity saves new messages that subscribers skip by pressing # during message playback as saved messages rather than as new messages. Subscribers in your organization may prefer this so that when they call Cisco Unity to check for new messages, they hear only newly arrived messages, and not the messages that they skipped earlier. Likewise, subscribers can then rely on their MWIs to determine when a new message arrives.

How Cisco Unity saves new messages that subscribers skip depends on the registry value you set:

0	Cisco Unity saves skipped messages as new messages.
1	Cisco Unity saves skipped messages as saved messages.

The registry change is applied system-wide to all subscribers who are associated with the Cisco Unity server and who use Optional Conversation 1. You cannot make the change for an individual subscriber or a specific group of subscribers who use Optional Conversation 1. The change does not affect subscribers who use the standard conversation.

Note If Cisco Unity failover is configured, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated

Do the following procedure if you would like Cisco Unity to save new messages as saved messages when subscribers skip them by pressing # during message playback. Note that the procedure does not change how Cisco Unity saves messages when subscribers press 9 or # after message playback.

To Change How Cisco Unity Handles Messages That Subscribers Skip By Pressing # During Message Playback

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Cisco Unity Settings pane, click **Optional Conversation 1: Customize Skipped Message State**.

Step 4 In the New Value list, click the applicable value, and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

Changing How Subscribers Confirm Message Addressing

The Cisco Unity subscriber conversation can be customized to alter how Cisco Unity prompts a subscriber to confirm message addressing. By default, when a subscriber addresses a message, Cisco Unity plays the recorded name and extension of the intended recipient (or, when there is no recorded name, Cisco Unity plays the extension instead) and asks the subscriber to confirm that the recipient is correct.

By using the Advanced Settings Tool to change the registry, you can customize how Cisco Unity prompts subscribers to confirm message addressing. Table 15-1 shows the confirmation prompts that subscribers hear during message addressing, depending on the registry value you set.

Note The Advanced Settings Tool also allows you to customize other aspects of the subscriber conversation. The Cisco Unity prompts listed in Table 15-1 assume that all other registry settings related to the subscriber conversation are set to their default values. Changes to some registry settings—such as the Directory List Selection Style setting—affect what the subscriber hears when you customize message addressing.

Table 15-1 Confirmation Prompts During Message Addressing

Registry Value	When There Is an Exact Match	When There Is More Than One Matching Name
0	"For <recipient name> at <extension>, press #. To cancel, press *."	"There are <x> matching names; choose by number. For Alex Campbell at extension 2015, press 1. For Li Campbell at extension 2003, press 2. For Terry Campbell at extension 2078, press 3..."
1	"For <recipient name>, press #. To cancel, press *."	"There are <x> matching names; choose by number. For Alex Campbell, press 1. For Li Campbell, press 2. For Terry Campbell, press 3..."
2	"Added."	"There are <x> matching names; choose by number. For Alex Campbell at extension 2015, press 1. For Li Campbell at extension 2003, press 2. For Terry Campbell at extension 2078, press 3..."

The registry change is applied system-wide to all subscribers associated with the Cisco Unity server. You cannot change how Cisco Unity prompts an individual subscriber or a specific group of subscribers to confirm message addressing.

Note If the Cisco Unity system is configured for failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

Do the following procedure to change how subscribers confirm message addressing.

To Change How Subscribers Confirm Message Addressing

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Subscriber Addressing Confirm Match Mode**.

Step 4 In the New Value list, click the applicable value, and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

You do not need to restart the Cisco Unity software for the registry change to take effect.

Changing How Subscribers Skip Messages During Message Playback (Standard Conversation)

You can customize the standard conversation to change how subscribers skip messages. By default, subscribers can press the # key to fast-forward to the end of a message, and press ## to skip to the next message as they play messages. You may want to consider changing the Cisco Unity conversation so that subscribers can press a single # key to skip a message during message playback.

By using the Advanced Settings tool to change the registry, you can specify what action Cisco Unity takes when subscribers press the # key while playing new, saved, and deleted messages. (Subscribers require the applicable COS rights to play deleted messages by phone.) The applicable registry values are:

0	When subscribers press the # key during message playback, Cisco Unity fast-forwards to the end of the message and then plays the After Message menu. Subscribers press ## to skip to the next message during message playback. (Default)
1	When subscribers press the # key during message playback, Cisco Unity skips to the next message. Cisco Unity skips two messages when subscribers press ## during message playback. Subscribers no longer have a way to fast-forward to the end of the message.

The registry change is applied system-wide to all subscribers who are associated with the Cisco Unity server and who use the standard conversation. You cannot use the Advanced Settings tool to make the change for an individual subscriber or a specific group of subscribers who use the standard conversation.

Before you set # to skip to the next message for all subscribers, carefully consider that subscribers will no longer have a way to fast-forward to the end of the message once you do. Changing whether subscribers press # or ## to skip a message during message playback also affects the shortcuts that subscribers can use while listening to a message. The changes to all keys are summarized in Table 15-2.

For this reason, we recommend that you use the Custom Keypad Map utility to adjust how # behaves during message playback so that you can map a key to allow subscribers to fast-forward to the end of the message at the same time. (You assign subscribers to a Custom Keypad Mapping conversation on the Subscribers > Subscriber > Conversation page in the Cisco Unity Administrator.) For additional information on using the utility, see the "Using the Custom Keypad Mapping Utility to Customize the Conversation" section on page 14-15.

Table 15-2 Shortcut Keys Affected by Changing How # Behaves During Message Playback

Task	Key(s) Subscribers Press When Registry Value Is 0[1]	Key(s) Subscribers Press When Registry Value Is 1
Skip message and save as is	##	#

Table 15-2 Shortcut Keys Affected by Changing How # Behaves During Message Playback

Task	Key(s) Subscribers Press When Registry Value Is 0[1]	Key(s) Subscribers Press When Registry Value Is 1
Fast-forward to end of message (Cisco Unity plays After Message menu)	#	<no keys mapped>
Fast-forward to end of message and restore as saved	#2	<no keys mapped>
Fast-forward to end of message and reply	#4	<no keys mapped>
Fast-forward to end of message and reply to all	#42	<no keys mapped>
Fast-forward to end of message and forward message	#5	<no keys mapped>
Fast-forward to end of message and save as new/restore as new	#6	<no keys mapped>
Fast-forward to end of message and deliver e-mail/fax to fax	#8	<no keys mapped>
Fast-forward to end of message and play message properties	#9	<no keys mapped>

1. Note that the *Cisco Unity at a Glance*, *Cisco Unity Phone Menus and Shortcuts*, and the *Cisco Unity User Guide* reflect the key mapping that subscribers use when the registry value is set to 0.

Finally, if subscribers in your organization are already accustomed to pressing ## to skip to the next message, review the "Support Desk Orientation" section on page 29-7 before you make the change. It is important that you understand the potential problems that may arise when subscribers do not readily adapt to the new key mappings.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated

Do the following procedure if you would like to change the action that Cisco Unity takes when subscribers press the # key during message playback.

To Change How Subscribers Skip Messages During Message Playback

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Set # to Skip to Next Message (Standard Conversation Only)**.

Step 4 In the New Value list, click the applicable value, and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Restart the Cisco Unity software for the registry change to take effect.

Changing What Subscribers Hear When They Manage Deleted Messages

You can use the Advanced Settings tool (available in Tools Depot) to customize the subscriber conversation to change what subscribers hear when they manage their deleted messages in the following ways:

- Change how Cisco Unity handles the way in which multiple deleted messages are permanently deleted. By default, when subscribers press 3 > 2 > 2 from the Main menu to permanently delete multiple deleted messages at once, Cisco Unity allows them to choose which messages they want to delete; subscribers can either delete their deleted voice messages or delete all of their deleted messages.

  As alternatives to the default, you can specify that Cisco Unity does not prompt subscribers to choose, and instead will permanently delete the type of messages you specify: either deleted voice messages or all deleted messages (voice, fax, and e-mail, as applicable). To set up either alternative, use the Advanced Settings tool to change the Conversation—Set How Deleted Messages Are Deleted in Bulk setting. See Advanced Settings Help for details.

- Enable Cisco Unity to request confirmation from subscribers before proceeding with a permanent deletion of a single deleted message. (To permanently delete a deleted message, subscribers must belong to a class of service that allows them to retain and review deleted messages.) By default, when subscribers permanently delete a deleted message as they review deleted messages by phone, Cisco Unity does not ask them to confirm the deletion.

  You can enable Cisco Unity to request confirmation from subscribers before proceeding with the deletion (use the Advanced Settings tool to change the Conversation—Confirm Delete When Deleting a Deleted Message setting; see Advanced Settings Help for details).

- Enable Cisco Unity to request confirmation from subscribers before proceeding with a deletion of a single new or saved message. By default, when subscribers delete a new or saved message, Cisco Unity does not ask them to confirm the deletion. You may want to enable Cisco Unity to request confirmation from subscribers before proceeding with the deletion, especially if many subscribers do not belong to a class of service that allows them to retain and review their deleted messages, because the deletion would be permanent for them.

Configuring Call Waiting Hold Time

With call holding, when the phone is busy, Cisco Unity can ask callers to hold. Cisco Unity manages each caller in the queue, according to the settings you configure. You can configure call waiting hold time, as described below. You can also customize the music that callers hear while on hold, as described in the "Working With Cisco Unity Music on Hold" section on page 11-5.

The call holding wait time for the first caller in the queue can be configured by making changes in the following registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\CallTransfer\1.0\WaitTimeSec

HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\CallTransfer\1.0\Attempts

The default value for each key is 5. To obtain the call holding queue wait time for the first caller in the queue, Cisco Unity multiplies the values of the keys. For example, the default value of 25 seconds is a WaitTimeSec of 5 seconds x 5 Attempts. If both keys were set to a value of 10, the call holding queue wait time would be 100 seconds (a WaitTimeSec of 10 x 10 Attempts), and so on.

The WaitTimeSec setting controls how long Cisco Unity waits between attempts to connect the caller. We recommend a value between 5 and 15. A value outside of this range could prevent Cisco Unity from functioning as designed.

The Attempts setting controls how many times Cisco Unity tries the subscriber extension before asking whether the caller wants to continue to hold. We recommend a value between 2 and 10. Increasing this setting will decrease the frequency at which Cisco Unity asks whether the caller wants to continue to hold.

If these registry keys are not present on your system, you can add them as DWORD values. You do not need to restart Cisco Unity for the changes to take effect.

Do the following procedure to add or change call holding wait time registry keys.

To Add or Change Call Holding Wait Time Registry Keys

Step 1 On the Cisco Unity server, on the Windows Start Menu, click **Run**.

Step 2 Start **Regedit**.

Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the "Restoring" topics in Registry Editor Help.) Note that when Cisco Unity failover is configured, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated. If you have any questions about changing registry key settings, contact Cisco TAC.

Step 3 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 4 Expand the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\CallTransfer\1.0**

If the registry key does not exist, continue with Step 5; otherwise, skip to Step 12.

Step 5 On the Edit menu, click **New Key**.

Step 6 Name the new key **CallTransfer**.

Step 7 Click the new **CallTransfer** key, then on the Edit menu, click **New Key**.

Step 8 Name the new key **1.0**.

Step 9 Click the new **1.0** key, then on the Edit menu, click **New DWORD Value**.

Step 10 Double-click the new **DWORD**.

Step 11 In the Edit DWORD Value window, name the new DWORD **WaitTimeSec**, and then click **Decimal**.

Step 12 Set the WaitTimeSec Value Data to a number between 5 and 15.

Step 13 Click **OK**.

Step 14 Expand the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\CallTransfer\1.0**

If the Attempts setting for the registry key does not exist, continue with Step 15; otherwise, skip to Step 18.

Step 15 Click the **1.0** key, then on the Edit menu, click **New DWORD Value**.

Step 16 Double-click the new **DWORD**.

Step 17 In the Edit DWORD Value window, name the new DWORD **Attempts**, and then click **Decimal**.

Step 18 Set the Attempts Value Data to a number between 2 and 10.

Step 19 Click **OK**.

Step 20 Close the Registry Editor.

Step 21 If the Cisco Unity system is configured for failover, repeat this procedure to apply the registry setting on the secondary server.

Enabling a Warning Tone for End of Recording

Note This feature does not apply to phone system integrations that use voice cards.

Cisco Unity can be set to sound a warning tone before reaching the maximum allowable message length while callers record their messages. By default, the warning tone is disabled. There are two settings that can be customized:

- The number of milliseconds before reaching the maximum message length when the warning tone will sound. Any setting greater than 0 enables the warning tone.
- The maximum recording length in milliseconds for which no warning tone will sound. This setting prevents the warning tone from sounding for shorter recordings such as voice names.

For example, if the maximum message length is set for 300 seconds and the first setting is set for 10 seconds, the warning tone will sound after 290 seconds of recording—10 seconds before the recording limit is reached and the recording session is terminated.

You can also customize the warning tone by recording a WAV file with another tone or a brief message. See the "Customizing the Warning Tone for End of Recording" section on page 15-9.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated

To enable the warning tone, do the following procedure.

To Enable the Warning Tone for the End of Recording

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Record Termination Warning: Record Termination Warning Time**. Information about this setting appears in the Description box.

Step 4 In the New Value field, enter a number of milliseconds to indicate when the warning tone will sound. The tone sounds this number of milliseconds prior to the end of the allowed recording time. We recommend entering **10000**.

Step 5 Click **Set**.

Step 6 In the Unity Settings pane, click **Conversation—Record Termination Warning: Minimum Recording Length for Termination Warning**.

Step 7 In the New Value field, enter the maximum recording length in milliseconds for which no warning tone will sound. We recommend entering **30000**.

Step 8 Click **Set**.

Step 9 Click **Exit**.

Step 10 For the settings to take effect, exit and restart the Cisco Unity software.

Customizing the Warning Tone for End of Recording

When enabled, a recording beep sounds as the warning tone. You can customize the warning tone by recording another tone or a brief message as a WAV file and specifying the location of the WAV file.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated

To Specify the Location of a Customized Warning Tone

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Record Termination Warning: Warning WAV File Location**.

Step 4 In the New Value field, enter the full path of the WAV file that you want to use as the warning tone.

Step 5 Click **Set**.

Step 6 Click **Exit**.

Step 7 For the settings to take effect, exit and restart the Cisco Unity software.

Configuring Cisco Unity Behavior for Replying to All Recipients of a Message

When a message is sent to multiple subscribers and/or distribution lists, the recipients have the option to reply to all recipients. The following default behavior should be noted:

- If the original message was sent to just one subscriber and he or she attempts to reply-all, Cisco Unity warns that the message has only one recipient and then plays the after-message menu again. Subscribers will hear "Reply-to-all is not available because the message has only one recipient."
- If the number of recipients on the original message is more than 50, Cisco Unity does not allow recipients to reply-all. Subscribers will hear "this message has too many recipients."
- If the original message includes at least one public distribution list, and the subscriber who is attempting to reply-all belongs to a COS that does not allow sending messages to public distribution lists, the subscriber will hear "This message has at least one distribution list as a recipient. You are not allowed to send messages to distribution lists."
- If a subscriber attempts to reply-all to a message that was from a remote subscriber or included some remote recipients, they will hear the prompt "Some recipients of the original message may not receive this reply."

By default, when a subscriber replies to all recipients of a message, Cisco Unity does not indicate to the subscriber how large the recipient list is. You can configure Cisco Unity to warn subscribers when the recipient list is greater than a certain number. See the following "To Configure Cisco Unity to Warn Subscribers When the Recipient List is Large" procedure. When the original message includes at least one public distribution list or if the number of recipients is equal to or greater than the number you specify, subscribers will hear "This reply-to-all contains many recipients. To continue recording, press 1. To review the original recipient list, 2. To cancel, press *."

To Configure Cisco Unity to Warn Subscribers When the Recipient List is Large

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Reply-to-All Warning.**

Step 4 In the New Value field, enter a number between 1 and 50. (If the number is set to zero, Cisco Unity will not warn subscribers.)

Step 5 Click **Set**.

Step 6 Click **Exit**.

Offering Live Record

Live record allows subscribers to record conversations while they talk to callers. The recorded conversation is stored as a message in the subscriber mailbox, and the subscriber can review it later or redirect it to another subscriber or group of subscribers. Operators in your organization may find live record particularly useful.

Live record is supported only when Cisco Unity is integrated with a Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) phone system. In addition, live record does not work for subscribers who have full mailboxes. When a subscriber who has a full mailbox records a call, the feature seems to work normally, but the recorded conversation is not stored as a message in the subscriber mailbox.

The Advanced Settings Tool allows you to specify how often Cisco Unity plays a beep as a call is recorded and how long the beep plays. To set up live record—including the beep, see the Cisco Unity Tools website at http://www.ciscounitytools.com/App_LiveRecord_405.htm.

DISCLAIMER: The use of monitoring, recording, or listening devices to eavesdrop, monitor, retrieve, or record phone conversations or other sound activities, whether or not contemporaneous with transmission, may be illegal in certain circumstances under federal, state and/or local laws. Legal advice should be sought prior to implementing any practice that monitors or records any phone conversation. Some laws require some form of notification to all parties to a phone conversation, such as by using a beep tone or other notification method or requiring the consent of all parties to the phone conversation, prior to monitoring or recording the phone conversation. Some of these laws incorporate strict penalties. In cases where local laws require a periodic beep while a conversation is being recorded, the Cisco Unity phone system provides a user with the option of activating “the beep.” Prior to activating Cisco Unity’s call record function, check the laws of all applicable jurisdictions. This is not legal advice and should not take the place of obtaining legal advice from a lawyer. IN ADDITION TO THE GENERAL DISCLAIMER THAT ACCOMPANIES THIS UNITY PRODUCT, CISCO ADDITIONALLY DISCLAIMS ANY AND ALL LIABILITY, BOTH CIVIL AND CRIMINAL, AND ASSUMES NO RESPONSIBILITY FOR THE UNAUTHORIZED AND/OR ILLEGAL USE OF THIS UNITY PRODUCT. THIS DISCLAIMER OF LIABILITY INCLUDES, BUT IS NOT NECESSARILY LIMITED TO, THE UNAUTHORIZED AND/OR ILLEGAL RECORDING AND MONITORING OF TELEPHONE CONVERSATIONS IN VIOLATION OF APPLICABLE FEDERAL, STATE AND LOCAL LAWS.

Setting Up System Transfers

In your organization, you may find that callers want to be able to dial numbers that are not typically listed in directory assistance. For example, subscribers and outside callers may find it convenient to be able to call Cisco Unity and transfer from the Opening Greeting or another call handler to a lobby extension, conference room extension, or an extension assigned to someone in the organization who is not a Cisco Unity subscriber, such as an employee who is visiting from another site and is using a guest office. In addition, some subscribers may want to be able to call Cisco Unity and then transfer to phone numbers outside of the organization—such as frequently called customers or vendors—so that they do not have to hang up after checking messages to place another call, or so that they will not incur long-distance charges while on business travel.

You can route callers to one of two "system transfer" conversations, both of which offer callers the ability to transfer to numbers that are not associated with Cisco Unity subscribers:

Caller System Transfer	This conversation prompts callers to enter the number that they want to transfer to. To protect Cisco Unity from toll fraud and unauthorized use, Cisco Unity performs the transfer only when the CS_Default_System_Transfer restriction table permits it.
Subscriber System Transfer	This conversation prompts callers to log on to Cisco Unity. After callers enter their Cisco Unity IDs and passwords, Cisco Unity prompts them to enter the number that they want to transfer to. To protect Cisco Unity from toll fraud and unauthorized use, Cisco Unity performs the transfer only when permitted by the transfer restriction table that is associated with the class of service for the subscriber who logged on.

You can route callers to either system transfer conversation in several ways, including:

- By offering a system transfer as a "one-key dialing" option. You can specify either system transfer (on the Caller Input page for any call handler or subscriber greeting) as the action that Cisco Unity performs when a caller presses a particular key during the greeting.

  For example, to allow all callers to transfer to a lobby phone, guest office, or a conference room from the Opening Greeting, you could specify that Cisco Unity will offer Caller System Transfers when callers press 3. To offer system transfers to a particular subscriber, you could specify that Cisco Unity will offer Subscriber System Transfers when the subscriber presses a particular key during the Opening Greeting or even during his or her own greeting.
- By creating a new phone number and a corresponding routing rule to send callers to either system transfer conversation. In this way, when callers dial the number, Cisco Unity sends calls to the system transfer conversation you specify.
- By creating a Custom Keypad Mapping conversation that maps a key to Subscriber System Transfers and offers it to subscribers in the main menu.

Note Regardless of how you offer callers either type of system transfer, Cisco Unity releases calls to the phone system, which handles the transfer to the specified number.

Follow the applicable task list in this section to set up Caller and Subscriber System Transfers. For both types of transfers, Cisco Unity prompts subscribers and callers to confirm the number that they enter before performing the transfer. To disable the confirmation prompt, use the Advanced Settings tool to change the Conversation—Confirm Number Before System Transfer Conversation setting. See Advanced Settings Help for details. (The Advanced Settings tool is available in Tools Depot.)

Task List: Offering Caller System Transfers

1. Modify the CS_Default_System_Transfer restriction table so that callers can dial numbers that you want to allow. See the "Managing Restriction Tables" chapter for details on how restriction tables work and how to modify them.
2. Set up a one-key dialing option or a new phone number that callers can use for system transfers:

- **Setting Up a One-Key Dialing Option**—Use caller input settings for a call handler to send callers to the Caller System Transfer conversation when they press the key that you specify during a call handler greeting. Then, enable caller input for the applicable greeting and re-record the greeting to mention the key that callers can press in the call handler greeting. (For example, "...to reach a conference room, press 3.") See the "Routing Callers by Using One-Key Dialing" section on page 3-2.
- **Setting Up a "System Transfers" Phone Number**—Refer to the documentation for the phone system to set up a new phone number. Then, on the Call Management > Call Routing > Direct Calls page in the Cisco Unity Administrator, create a routing rule that sends any call that arrives for the new number to the Caller System Transfer conversation. Distribute the new number to callers who will find Caller System Transfers convenient. See the "Creating and Modifying Call Routing Rules" section on page 3-5 for details on creating routing rules for direct calls.

Task List: Offering Subscriber System Transfers

1. For the subscribers who will use Subscriber System Transfers, modify the transfer restriction table that is associated with the subscriber class of service so that the subscribers can dial numbers that are not associated with Cisco Unity entities. See the "Managing Restriction Tables" chapter for details on how transfer restriction tables work and how to modify them to allow the numbers you want.

Tip If you are not offering system transfers to all subscribers in a single class of service, reassign those who will use it to a new class of service that has a transfer restriction table that will allow them to dial the applicable numbers.

2. Set up a one-key dialing option, a Custom Keypad Mapping conversation, System Transfers, or a new phone number that callers can use for system transfers:
   - **Setting Up a One-Key Dialing Option**—Use caller input settings for a call handler or a subscriber greeting to send callers to the Subscriber System Transfer conversation when they press the key that you specify during the greeting. Then, enable caller input for the applicable greeting. Tell subscribers which key to press to access the Subscriber System Transfer conversation when they listen to the greeting, or if you are not concerned about other callers hearing the option and not being able to use it, re-record the greeting to mention the key. (For example, "...to reach a conference room, press 3.") See the "Routing Callers by Using One-Key Dialing" section on page 3-2.
   - **Setting Up a Custom Keypad Mapping Conversation**—Refer to the documentation for using the Custom Key Map Utility. Add Subscriber System Transfer to the options offered to subscribers at the main menu. Then, configure subscribers to use the Custom Keypad Mapping conversation. See the "Using the Custom Keypad Mapping Utility to Customize the Conversation" section on page 14-15.
   - **Setting Up a "System Transfers" Phone Number**—Refer to the documentation for the phone system to set up a new phone number. Then, on the Call Management > Call Routing > Direct Calls page in the Cisco Unity Administrator, create a routing rule that sends any calls to the new number to the Subscriber System Transfer conversation. Distribute the new number only to the subscribers who will use Subscriber System Transfers. See the "Creating and Modifying Call Routing Rules" section on page 3-5 for details on creating routing rules for direct calls.

Enabling Alternate Greeting Notices

Because subscribers never hear the greetings of their message recipients when they send, reply to, and forward messages, consider enabling "alternate greeting notices" for the Cisco Unity server so that subscribers are alerted when a message recipient has the alternate greeting enabled. Alternate greeting notices are a type of message receipt. When a subscriber leaves or sends a message to a subscriber who has the alternate greeting enabled, Cisco Unity delivers the message and also sends the sender an alternate greeting notice. The alternate greeting notice says:

> "The alternate greeting for <subscriber name or ID> is on and will remain on until <expiration date for the greeting>. The message you sent was delivered, but the recipient may not be available to play it."

When the greeting is set to play indefinitely, Cisco Unity will indicate that rather than play an expiration date.

An alternate greeting notice is sent in response to the first message that a subscriber leaves or sends to a recipient within the time period that the recipient has the alternate greeting enabled. If the subscriber leaves or sends subsequent messages to the same recipient, Cisco Unity does not respond with additional notices (unless the recipient turns off the alternate greeting and then enables it again).

When the feature is enabled, subscribers can play notices by phone or they can view the text from the Cisco Unity Inbox, assuming that they can access receipts (you can disable receipts per server by using the Advanced Settings Tool). Though alternate greeting notices are automated responses, they are from the message recipient. Thus, subscribers can use the Message Locator to find both messages and notices from a particular subscriber. Note that like other types of receipts, alternate greeting notices do not trigger message waiting indicators (MWIs).

Cisco Unity does not send notices in response to system broadcast messages, nor does it send notices to unidentified callers. Cisco Unity sends a notice to the sender when the message is addressed to an individual subscriber or to a distribution list of which the recipient is a member. Notices are sent regardless of whether the sender and recipient are homed on the same Cisco Unity server or are on separate servers that are digitally networked (assuming that the feature is enabled for each server). However, when other networking features (AMIS, Bridge, or VPIM) are used, subscribers do not receive notices in response to messages left for or sent to remote Cisco Unity or Cisco Unity Express subscribers, nor do they receive notices in response to messages left for or sent to remote users on a another voice messaging system—even when the recipients have their alternate greeting or similar type of greeting (such as an extended absence greeting) enabled.

Alternate greeting notices are disabled by default. You can enable alternate greeting notices only per server; you cannot specify that notices are sent only to certain subscribers or only in response to messages sent by certain subscribers. In digitally networked environments, the feature should be enabled for all Cisco Unity servers in the network.

To set up the Cisco Unity server to send a notice to subscribers when they leave, send to, reply to, or forward messages to other subscribers who have their alternate greeting enabled, do the following "To Enable Alternate Greeting Notices for a Cisco Unity Server" procedure. Note that when you do the procedure, Cisco Unity will not send notices in response to messages sent to subscribers who already had their alternate greeting enabled before you finished the procedure.

If you later choose to disable alternate greeting notices, any existing notices in subscriber mailboxes will no longer be available to subscribers until you enable the feature again, and subscribers will no longer receive notices—even if other Cisco Unity servers in the network have the feature enabled.

Due to conflicts with the "Out of Office" rule in Outlook, enabling alternate greeting notices for Unified Messaging systems is not supported.

To Enable Alternate Greeting Notices for a Cisco Unity Server

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Alternate Greeting Notices**.

Step 4 In the New Value list, click **1** and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Restart the **Cisco Unity** software.

Note If you do not restart the Cisco Unity software when you enable or disable the feature, notices do not behave as expected.

Step 8 As applicable, repeat the procedure for each Cisco Unity server at your site.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

Simulating Abbreviated Extensions

You can simulate abbreviated extensions by using prepended and postpended digits for call handlers and subscriber mailboxes. When such digits are defined, they will be prepended and postpended to any extension that a caller dials while listening to the greeting for the call handler or subscriber mailbox.

Cisco Unity first attempts to route the call to the prepended/postpended extension. If the prepended/postpended extension is not valid, Cisco Unity attempts to route the call to the dialed extension. For example, a call handler named Sales is configured with the prepended digits 123 and the postpended digits 456. When a caller dials 1000 while listening to the greeting for the Sales call handler, Cisco Unity attempts to route the call to extension 1231000456; if the prepended/postpended extension is not valid, Cisco Unity attempts to route the call to extension 1000.

You can set up multiple call handlers for which callers are able to enter the same digits (for example 1000) to reach a support person, but the calls can be routed to a support person appropriate to the particular call handler (for example, a Technical Support call handler or a Sales call handler) because of the presence of the prepended and postpended digits.

To enable and configure abbreviated extensions, do the following two procedures:

- To Enable Simulated Abbreviated Extensions, page 15-15
- To Configure Prepended and Postpended Digits for Subscribers or Call Handlers, page 15-16

To Enable Simulated Abbreviated Extensions

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Administration—Expose Prepend and Postpend Digits for Call Handlers and Subscribers**.

Step 4 In the New Value list, click **1**, and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

You do not need to restart Cisco Unity for the change to take effect.

To Configure Prepended and Postpended Digits for Subscribers or Call Handlers

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Caller Input** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber account. Then browse to the **Caller Input** page.
- To modify a call handler, go to any **Call Management > Call Handlers** page and find the applicable call handler. Then browse to the **Caller Input** page.

Step 2 Enter values in the **Prepend Digits** and the **Postpend Digits** fields as applicable.

Step 3 Click the **Save** icon.

CHAPTER 16

Managing Conversation Settings That Are Controlled by Class of Service

See the following sections:

Enabling Live Reply

When live reply is enabled, subscribers who are listening to messages by phone can reply to a subscriber message by pressing 4-4 to have Cisco Unity call the subscriber. (Subscribers who use Optional Conversation 1 press 8-8 for live reply.) For single-server installations, Cisco Unity dials the extension of the subscriber who left the message only when the Transfer Incoming Calls to Subscriber's Phone setting for the subscriber who left the message is set to ring an extension or another number. (The Transfer Incoming Calls to Subscriber's Phone field is on the Subscribers > Subscribers > Call Transfer page in the Cisco Unity Administrator.) In addition, the call transfer settings for the subscriber who left the message dictate what Cisco Unity does when the subscriber phone is busy, and whether Cisco Unity screens the call.

When subscribers use the live reply feature to return a call from a subscriber and then leave a message for the subscriber that they called, Cisco Unity uses the calling number to identify who the message is from. This means that Cisco Unity can correctly identify who the message is from only when a subscriber uses live reply from his or her own extension. However, when a subscriber uses another phone to use live reply and leave a message for a subscriber, Cisco Unity does not correctly identify who the message is from. Instead, Cisco Unity may indicate that the message is from an "unidentified caller" even though the subscriber who left the message was logged on to Cisco Unity at the time.

Note By default, live reply is restricted to subscribers on the same Cisco Unity server. If your installation consists of multiple networked Cisco Unity servers, there are additional configuration steps required to enable live reply to a subscriber on another Cisco Unity server. For more information, see the "Enabling Live Reply Between Cisco Unity Servers in the Same Dialing Domain (Optional)" section in the "Digital Networking" chapter of the applicable *Networking Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Consider informing subscribers when you enable this feature, because even when it is enabled, the live reply option is not mentioned in the main Cisco Unity phone menus. It is mentioned in the Help menu for the Cisco Unity phone conversation, the *Cisco Unity User Guide*, and the *Cisco Unity at a Glance*.

Enabling a Post-Greeting Recording

You can use the settings on the applicable Subscribers > Class of Service > Greetings page in the Cisco Unity Administrator to specify whether Cisco Unity plays a recording before allowing callers to leave a message for subscribers who are assigned to a class of service (COS). For each COS, you use the Media Master control bar on the page to record what you want callers to hear, and you indicate whether all callers hear the recording or only unidentified callers. Though callers can press # to skip a subscriber or call handler greeting, callers cannot skip a post-greeting recording.

When Cisco Unity is enabled to play a post-greeting recording, callers hear the recording immediately after a subscriber greeting, regardless of which personal greeting is enabled for the subscriber. The post-greeting recording also plays after a call handler greeting when the call handler is configured to take a message and the message recipient for the call handler is a subscriber who is assigned to a COS that has the recording enabled. (The COS assigned to the owner of a call handler has no effect on whether the recording is played.)

By default, the post-greeting recording feature is disabled for all classes of service. Depending on your organization and the type of subscriber accounts that are assigned to each COS, you may want to consider enabling it for some classes of service, so that those who call certain groups of subscribers—such as a sales team, technical support group, or a Human Resources department—hear the recording. For each COS, you can create a different recording tailored to certain callers and as applicable, in an appropriate language. The recording can be up to 90 seconds in length.

For example, you may want to enable a post-greeting recording for a particular COS to convey a confidentiality policy or to let callers know when they can expect a response to the message. You can also use the feature to remind callers to include contact information, invoice or policy numbers, and other such information when they leave messages. Conversely, due to legal or security concerns, you may want to advise callers of what information not to include in messages—information like passwords, financial transaction requests, and so on.

A post-greeting recording does not play when:

- The message recipient for a call handler is assigned to a distribution list.
- Subscribers send, reply to, or forward messages to other subscribers, and when subscribers call a subscriber extension, log on to Cisco Unity during the subscriber greeting, and then leave a message.

Note When you create a new COS based on an existing one, the new COS inherits the post-greeting recording settings but not the recording itself.

Do the following procedure to enable a post-greeting recording for a class of service. Whether you plan to enable the feature for a new COS or an existing one, consider testing the feature by enabling it for a new COS that has a test subscriber account assigned to it. In this way, you can call the test subscriber to hear how your recording will sound after the greeting and can adjust what you plan to say.

To Enable a Post-Greeting Recording for a Class of Service

Step 1 In the Cisco Unity Administrator, go to the applicable **Subscribers > Class of Service > Greetings** page.

Step 2 In the After Greeting, Play Recording Before Taking Messages section, select one of the following options to enable the feature and indicate which callers will hear the recording:

- **Play Recording Only for Unidentified Callers**—Before they leave a message, outside callers and subscribers who did not log on to Cisco Unity before calling from an external phone or from a phone that is not associated with a subscriber account hear the subscriber or call handler greeting and then the recording.
- **Play Recording to All Callers**—Before they leave a message, subscribers and outside callers hear subscriber or call handler greeting and then the recording.

Step 3 Use the Media Master control bar to record what you want callers to hear, or specify an existing WAV file as the recording.

(You use the Copy/Paste From File options on the Options menu of the Media Master control bar to use a prerecorded WAV file as the recording.)

Step 4 Click the **Save** icon.

CHAPTER 17

Managing Conversation Settings That Are Controlled by Subscriber or Subscriber Template Settings

See the following sections in this chapter:

Adjusting Response Timeouts for Phone Menus

For each subscriber, you can specify the following timeout settings for responding to phone menus:

- How long Cisco Unity waits for the subscriber to press a key after playing a menu.

- How long Cisco Unity waits for additional key presses after the subscriber has pressed a key to enter subscriber names or extensions, to address a message, to update passwords, to change call transfer or message notification numbers, and so on.
- How long Cisco Unity waits for additional key presses after the subscriber has pressed a key that represents the first digit of more than one possible key combination in a particular phone menu. (For example, in the After Message menu for the standard conversation, subscribers can press 4 to reply to a message, 42 to reply to all, or 44 to call the subscriber.) This also applies when using ## to switch addressing modes.
- How many times Cisco Unity repeats a menu if the subscriber has not responded.

To adjust the response timeout setting, do one of the following two procedures:

- To Adjust the Timeout Settings for Menu Responses for Individual Subscribers, page 17-2
- To Change the Timeout Settings for Outside Callers and All Subscribers, page 17-3

You can also change these settings for a group of subscribers by using the Bulk Edit utility, and subscribers can adjust this setting themselves on the Advanced Settings page in the Cisco Unity Assistant.

To Adjust the Timeout Settings for Menu Responses for Individual Subscribers

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Modify the following fields, as applicable:

- **After Playing a Menu, Wait <x> Milliseconds for Subscriber to Press the First Key**.
- **Wait <x> Milliseconds for Additional Key Presses When Entering Names and Numbers.**
- **Wait <x> Milliseconds for Additional Key Presses When Entering Phone Menu Commands.** We recommend that you keep the response timeout value for menu commands between 750 and 2,000 milliseconds. Longer timeouts can result in frustrating delays for subscribers, while shorter timeouts may not leave subscribers with enough time to press all intended digits.
- **If Subscriber Does Not Respond to a Menu, Repeat Menu <x> Times.** Use caution when significantly increasing the number of times that Cisco Unity repeats a menu for subscribers. In the event that a subscriber puts a call to Cisco Unity on hold and forgets to return to it, or if the call is not disconnected as expected when the subscriber hangs up, Cisco Unity can tie up a voice port for long periods of time by repeating a phone menu.

Note When you leave these fields blank, the settings specified on the System > Configuration > Settings page dictate how long Cisco Unity waits for subscribers and how many times Cisco Unity repeats a menu.

Step 3 Click the **Save** icon.

To Change the Timeout Settings for Outside Callers and All Subscribers

Step 1 In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page

Step 2 Modify the following fields, as applicable:

- **After Playing a Menu, Wait <x> Milliseconds for Subscriber to Press the First Key**.
- **Wait <x> Milliseconds for Additional Key Presses When Entering Names and Numbers.**
- **Wait <x> Milliseconds for Additional Key Presses When Entering Phone Menu Commands.** We recommend that you keep the response timeout value for menu commands between 750 and 2,000 milliseconds. Longer timeouts can result in frustrating delays for subscribers, while shorter timeouts may not leave subscribers with enough time to press all intended digits.
- **If Subscriber Does Not Respond to a Menu, Repeat Menu <x> Times.** Use caution when significantly increasing the number of times that Cisco Unity repeats a menu for subscribers. In the event that a subscriber puts a call to Cisco Unity on hold and forgets to return to it, or if the call is not disconnected as expected when the subscriber hangs up, Cisco Unity can tie up a voice port for long periods of time by repeating a phone menu.

Note Subscribers who have already had their timeout values adjusted on their individual Subscribers > Subscribers > Conversation page are not affected by changes made on the System > Configuration > Settings page.

Step 3 Click the **Save** icon.

Allowing Subscribers to Access Cisco Unity by Phone Without Entering a Password

By default, subscribers are prompted for a password before they can log on to Cisco Unity to check messages or change their personal settings. As a convenience to subscribers who often access Cisco Unity from a mobile phone, home phone, or phone in a secured office within your organization, you may consider specifying that Cisco Unity should not prompt them to enter a password when they call Cisco Unity to access their mailbox from their primary extension or alternate devices. (When they call Cisco Unity from an unknown extension, Cisco Unity will prompt them for their passwords as usual.)

Note For security reasons, it may not be appropriate to allow subscribers who work in shared workspaces, cubicles, or other public areas in your organization (such as a lobby or reception area) to access Cisco Unity by phone without first entering a password.

Do the following "To Allow Subscribers to Access Cisco Unity by Phone Without Entering a Password" procedure to allow an individual subscriber to access messages by phone without entering a password when they call from their primary extension or an alternate device. Subscribers who do not have to enter a password to log on to Cisco Unity are still prompted to renew their phone passwords when they expire.

To allow a group of subscribers to access Cisco Unity by phone without entering a password, use the Bulk Edit tool available in Tools Depot.

To Allow Subscribers to Access Cisco Unity by Phone Without Entering a Password

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Phone Password** page.

Step 2 In the Prompt for Phone Password section, check the **Only When User Calls From Unknown Extension** check box.

Step 3 Click the **Save** icon.

Asking Subscribers to Confirm Deletions of New and Saved Messages

By default, when subscribers delete new and saved messages by phone, Cisco Unity does not ask them to confirm the deletion. Some subscribers may prefer that Cisco Unity ask them to confirm the choice before deleting the messages. Confirming the deletion of messages is particularly useful to those subscribers who do not have access to deleted messages.

To specify that Cisco Unity will ask subscribers to confirm their deletions, do the following "To Specify That Cisco Unity Will Ask Subscribers to Confirm Deletions of New and Saved Messages" procedure for an individual subscriber or on a subscriber template. (To make the change for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.)

To Specify That Cisco Unity Will Ask Subscribers to Confirm Deletions of New and Saved Messages

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **Confirm Deletions of New and Saved Messages** check box.

Step 3 Click the **Save** icon.

Changing the Order for Addressing and Recording

The Cisco Unity subscriber conversation can be customized to change the order in which Cisco Unity prompts subscribers to address and record when they send or forward messages to other subscribers or distribution lists. By default, when a subscriber sends or forwards a message, Cisco Unity first prompts the subscriber to address the message and then prompts the subscriber to record the message or to record an introduction for a forwarded message.

Note that you cannot change the order in which Cisco Unity prompts subscribers to address and record when they reply to messages; Cisco Unity always prompts subscribers to record a reply before allowing them to add additional recipients.

You can also change this setting by using the Bulk Edit utility, and subscribers can enable and adjust the settings themselves on the Phone Menu Preferences page in the Cisco Unity Assistant.

To Change the Order for Addressing and Recording

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check or uncheck the **Address Message, Then Record It** check box, depending on the desired behavior.

Step 3 Click the **Save** icon.

Enabling Callers to Transfer From Subscriber Greetings to an Alternate Contact Number

As a convenience to callers, you can set up Cisco Unity so that callers can transfer to an alternate contact number by pressing a key during the greetings for a particular subscriber or a group of subscribers. An alternate contact number can be the extension for an operator or another subscriber (such as a supervisor or coworker), or any other number where the subscriber or another person can be reached.

You can use the Cisco Unity Administrator or the Bulk Edit utility to specify the key that callers press to transfer and the number that they transfer to. You can specify the same key and alternate contact number for multiple subscribers, or you can specify a different key and/or alternate contact number for each subscriber. Subscribers can specify the alternate contact number by using the Cisco Unity conversation or the Cisco Unity Assistant. (Note that the option to specify an alternate contact number appears in the Cisco Unity Assistant regardless of whether you have specified a key that callers can press to transfer from the subscriber greeting.) The alternate contact number is limited to the numbers allowed by the restriction table for transfers that is associated with the subscriber who specifies it.

When you enable the feature, you may want to specify the key(s) that can be used to make the transfer and leave the alternate contact number unspecified, so that subscribers can specify the number themselves. Until an alternate contact number is specified, Cisco Unity ignores the key set to transfer the call if callers happen to press it during a subscriber greeting. Because neither the Cisco Unity conversation nor the Cisco Unity Assistant indicate the key that you specified to allow callers to make the transfer, let subscribers know the key so that they can include the information in their greetings. When transferring a caller to an alternate contact number, by default Cisco Unity releases the call to the phone system. Alternatively, you can configure Cisco Unity to use the subscriber's active transfer rule settings, including call holding and call screening options.

Do the following "To Enable Callers to Transfer From Subscriber Greetings to an Alternate Contact Number" procedure to enable callers to transfer to an alternate contact number from a subscriber greeting. You can set up the feature to work for the greetings for an individual subscriber or for those subscribers who are associated with a subscriber template. Alternatively, you can use Bulk Edit to set up the feature for the greetings of multiple subscribers at once.

To Enable Callers to Transfer From Subscriber Greetings to an Alternate Contact Number

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Caller Input** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Caller Input** page.

Step 2 Select a key from the Caller Input Map or from the keypad.

Step 3 In the action section, click **Send Caller To** and then click **Alternate Contact Number**.

Step 4 In the Number to Dial field, enter digits 0 through 9 to specify an alternate contact number up to 30 digits in length. You can also enter:

- **,** (comma) to insert a one-second pause.
- **#** and ***** to correspond to the # and * keys on the phone.

Do not use spaces, dashes, or parentheses between digits. Begin with an access code, if needed to make an external call (for example, 9). For long-distance numbers, also include 1 and the area code.

Step 5 Indicate whether to lock the key to that action.

Step 6 Click the **Save** icon.

By default, Cisco Unity uses a release transfer when transferring callers to an alternate contact number. Alternatively, you can configure Cisco Unity to use the subscriber active transfer rule settings, including call holding and call screening options. Cisco Unity will still use the number for the transfer that is specified on Alternate Contact Number, but the transfer settings (release, supervised, call holding, and so on) come from the active transfer rule.

To Configure Cisco Unity to Use the Active Transfer Rule for Transfers to Alternate Contact Numbers

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—ACN Follows Current Transfer Rule.**

Step 4 In the New Value field, select **1**. (If the value is set to zero, Cisco Unity will always use a release transfer.)

Step 5 Click **Set**.

Step 6 Click **Exit**.

Handling Messages That Are Interrupted by Disconnected Calls

You can customize how Cisco Unity handles disconnected calls. Calls can be intentionally or unintentionally disconnected—for example, when a subscriber hangs up or when a cell phone loses its charge or signal.

- If the disconnect occurs while subscribers are in the process of sending, replying to, or forwarding messages, you can specify whether a message is sent or discarded. For more details, see the "Specifying Whether Messages Are Sent Upon Hang-Up" section on page 17-7.
- If the disconnect occurs while subscribers are in the process of listening to new messages, you can specify whether a message stays new or is marked as saved. For more details, see the "Specifying That Messages Are Marked Saved When Subscribers Hang Up or Are Disconnected" section on page 17-8.
- If the disconnect occurs while subscribers are either listening to or sending messages, you can enable Dropped Call Recovery, which allows subscribers to call back into Cisco Unity within a specified period of time and resume the activity without losing their place. For more details, see the "Dropped Call Recovery" section on page 17-8.

Specifying Whether Messages Are Sent Upon Hang-Up

You can change how Cisco Unity handles messages that are interrupted by disconnected calls while subscribers are in the process of sending, replying to, or forwarding messages. By default, Cisco Unity sends a message when the call is disconnected in the following circumstances:

When a subscriber is replying to or sending a message	As long as the message has at least one recipient and the recording is more than one second (1,000 ms) in length. This means that Cisco Unity sends the message even though the subscriber may not have finished recording or addressing the message.
When a subscriber is forwarding a message	As long as the message has at least one recipient. This means that Cisco Unity sends the message even though the subscriber may not have recorded an introduction or completely addressed the message.

By adjusting the default value of the setting, you can alter Cisco Unity behavior so that Cisco Unity will not send messages unless subscribers have pressed # to confirm that they are ready to send the message. Thus, if the call is disconnected before a subscriber has a chance to confirm, Cisco Unity deletes the message rather than sending it.

Note that if the subscriber has dropped call recovery enabled for calls dropped while addressing or recording messages, messages that are sent upon hang-up will not be sent until the time period for dropped call recovery has expired.

You can also change this setting by using the Bulk Edit utility, and subscribers can adjust the message addressing order themselves on the Phone Menu Preferences page in the Cisco Unity Assistant.

Note This setting does not apply to messages left by outside callers.

To Specify Whether Messages Are Sent Upon Hang-Up

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check or uncheck the **Send Message When Subscriber Hangs Up or Call Is Disconnected** check box, depending on the desired behavior.

Step 3 Click the **Save** icon.

Specifying That Messages Are Marked Saved When Subscribers Hang Up or Are Disconnected

By default, when subscribers listen to a message by phone, Cisco Unity retains the message as-is—either as a new or saved message—unless subscribers indicate otherwise before hanging up or being disconnected. However, some subscribers may prefer that Cisco Unity marks all messages saved as soon as they access the message.

Note that if the subscriber has dropped call recovery enabled for calls dropped during message playback and messages are configured to be marked as saved upon hang-up or disconnection, messages will remain "new" until the recovery timeout period for dropped call recovery has expired.

To specify that messages are marked saved when subscribers hang up or are disconnected, do the following "To Specify That Messages Are Marked Saved When Subscribers Hang Up or Are Disconnected" procedure for an individual subscriber or in a subscriber template. (To make the change for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.)

After you enable the feature, make sure to alert subscribers of the change.

To Specify That Messages Are Marked Saved When Subscribers Hang Up or Are Disconnected

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **Mark a Message as Saved Upon Hang-Up or Disconnection** check box.

Step 3 Click the **Save** icon.

Dropped Call Recovery

If subscribers inadvertently disconnect while listening to or sending messages, Dropped Call Recovery allows them to call back into Cisco Unity within a specified period of time and resume the activity without losing their place. By default, Dropped Call Recovery is not enabled.

When Dropped Call Recovery is enabled for a subscriber during message playback, the setting applies when the call terminates while the subscriber is listening to new or saved messages. It does not apply when the subscriber is listening to deleted messages or receipts, or when the subscriber is listening to messages by using the dynamic Message Locator option. By default, the recovery time period for calls dropped during message playback is five minutes. If the subscriber calls back during the specified period of time, he or she will be able to continue listening to the message. Note that if the Mark a Message as

Saved Upon Hang-Up or Disconnection option is also enabled for a subscriber, and the subscriber is disconnected while listening to a new message, the message will remain marked as new until the recovery time period has expired.

When Dropped Call Recovery is enabled for calls that are dropped while the subscriber is addressing or recording messages, the setting applies when the call terminates while the subscriber is sending a new message, replying to a message, or forwarding a message. If the message has at least one addressee or a recording and there is a disconnect, it will be held for the specified period of time before sending. By default, the recovery time period for calls dropped while addressing or recording messages is three minutes. If the subscriber calls back into the mailbox during that time, he or she will be offered the option to review the message, cancel it, or send it as is. If the subscriber does not call back during that time and the message has at least one addressee and a recording, the message will be sent only if the subscriber has the Send Message When Subscriber Hangs Up or Call Is Disconnected option enabled. If the Send Message When Subscriber Hangs Up or Call Is Disconnected option is not enabled, the message will be discarded.

You can also enable Dropped Call Recovery by using the Bulk Edit utility, and subscribers can enable and adjust the Dropped Call Recovery settings themselves on the Advanced Settings page in the Cisco Unity Assistant.

To Enable Dropped Call Recovery

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 To enable Dropped Call Recovery for calls that are dropped during message playback, check the **Enable DCR for Calls Dropped During Message Playback** check box, and if applicable, change the recovery period time.

Step 3 To enable Dropped Call Recovery for calls dropped while addressing or recording messages, check the **Enable DCR for Calls Dropped While Addressing or Recording Messages** check box, and if applicable, change the recovery period time.

Step 4 Click the **Save** icon.

Considerations for Using Dropped Call Recovery

The following behavioral notes should be considered when using the Dropped Call Recovery feature:

- If subscribers tend to “type ahead” by choosing menu options before they are prompted, they may skip past the Dropped Call Recovery options, which would be the same result as choosing the cancel option. When using this feature, subscribers can press the # key to go directly to the Dropped Call Recovery options. If there is no dropped call to recover, they will be taken to the main menu.
- When Dropped Call Recovery is enabled for calls that are dropped while addressing or recording messages, there could be a perception of delays when sending messages. If subscribers terminate message recordings by hanging up rather than explicitly sending messages by pressing the # key, their messages will not be sent until after the recovery timeout period has expired. For this reason, we recommend a recovery time period of three minutes.

- When Dropped Call Recovery is enabled for calls that are dropped while addressing or recording messages, the setting does not apply to messages left by using the Identified Subscriber Messaging (ISM) feature. (ISM is in effect when subscribers call other subscribers from their primary or alternate extensions and are forwarded to the greetings of the subscribers that they call.) Dropped Call Recovery only applies when subscribers log on to their voice mailboxes first and then address messages to other subscribers.
- When Dropped Call Recovery is enabled for calls that are dropped during message playback, and when messages are configured to be marked as saved upon hang-up or disconnection, messages will remain "new" until the recovery timeout period has expired. This may lead to the perception of a delay in turning off message waiting indicators.

Logging On to Cisco Unity From Subscriber Greetings

Caller input settings allow you to specify how subscribers log on to Cisco Unity when they are listening to a subscriber greeting. By using the caller input settings you can 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.

Note You specify caller input settings on the subscriber template and on individual subscriber pages in the Cisco Unity Administrator, or by using Bulk Edit or the Cisco Unity Bulk Import wizard. Caller input settings work for a particular greeting only when the Allow Caller Input check box is checked on the applicable Greetings page for the subscriber template or individual subscriber in the Cisco Unity Administrator.

By default, Cisco Unity is set up so that subscribers hear the Cisco Unity Sign-In conversation, which prompts them for their ID and password when they press * during any subscriber greeting—either their own or another subscriber greeting. As an alternative, you can accommodate subscribers who want an easier way to log on from their own greeting by offering the Easy Sign-In conversation, which prompts subscribers only for a password.

Table 17-1 summarizes the options available to you for specifying how subscribers log on to Cisco Unity from their own greeting or from another subscriber greeting.

Table 17-1 Summary of Caller Input Options Available for Specifying How Subscribers Log On to Cisco Unity from Subscriber Greetings

Cisco Unity Conversation	Description	Subscriber Use	Best Practice
Sign-In	Prompts subscribers to enter an ID and password when they press * during any subscriber greeting. Enabled by default.	To avoid leaving a message as "an unidentified caller," subscribers can log on to Cisco Unity from another subscriber greeting when they call the subscriber from a phone that is not associated with their account. (Cisco Unity subscribers cannot reply to messages from unidentified callers.)	Continue to offer the Sign-In conversation so that subscribers can make the most of identified subscriber messaging. If you are considering reassigning the key used to access the Sign-In conversation, consider that subscribers also access the Sign-In conversation by pressing * from the Opening Greeting.

Table 17-1 Summary of Caller Input Options Available for Specifying How Subscribers Log On to Cisco Unity from Subscriber Greetings (continued)

Cisco Unity Conversation	Description	Subscriber Use	Best Practice
Easy Sign-In	Prompts subscribers to enter a password when they press a key during any subscriber greeting. Disabled by default. (No key is mapped to the Easy Sign-In conversation.)	Subscribers can dial their extensions and log on quickly. In this situation, subscribers may prefer the Easy Sign-In to the Sign-In conversation for several reasons: • They find the extra step of entering their ID redundant as they had already entered it when they dialed their extension (assuming that Cisco Unity IDs are the same as subscriber extensions). • They find the extra step of entering their ID annoying because they migrated from another voice messaging system that did not prompt them to enter an ID when they logged on from their greeting. • They migrated from another voice messaging system and are used to pressing a different key to log on from their greeting. Offering subscribers a fast and familiar way to log on from their own greeting is a handy alternative when subscribers cannot remember the pilot number to access Cisco Unity by phone. (Note that when subscribers call another subscriber and attempt to log on, Cisco Unity requires the password associated with the extension of the subscriber who placed the call.)	Provide Easy Sign-In to subscribers who want a faster way to log on from their own greeting or to accommodate subscribers who are accustomed to another voice messaging system. Keys 1–9 are unmapped, and are therefore good choices for assigning to the Easy Sign-In conversation. Consider the following if you are thinking of using the *, 0, or # key instead: • Avoid reassigning the * key so that you can continue to offer the Sign-In conversation. • The # key is already set up to skip greetings. • The 0 key is already set up to send callers to the Operator call handler. • The Cisco Unity subscriber documentation reflects the behavior described above for the *, 0, and # keys.

Offering Subscribers Additional Caller Information Before Message Playback

The Cisco Unity subscriber conversation can be customized so that it provides subscribers with additional information about each caller who left a message, before it plays the message. By using the Bulk Edit utility (available in Tools Depot), you can provide individual subscribers or a specific group of subscribers with additional information on one or both of the types of callers who leave messages for them, as indicated in Table 17-2.

Table 17-2 Caller Information That Cisco Unity Can Offer Before Message Playback

For Messages Left By This Type of Caller	Message Type	Cisco Unity Plays This by Default	Cisco Unity Plays This When Additional Caller Information Is Offered
Identified subscriber (including call handlers)	Voice, fax, e-mail, receipts	The recorded name of the subscriber. If the subscriber (or call handler) does not have a recorded name, Cisco Unity plays the primary extension associated with the subscriber or call handler instead.	Both the recorded name (if available) and the primary extension before playing the message. When a subscriber (or call handler) does not have a recorded name nor an extension, Cisco Unity simply plays the message without announcing who it is from.
Unidentified caller	Voice	The message, without announcing who it is from or playing the phone number of the caller first.	The phone number (if available) of the caller before playing the message.

If you choose to provide Cisco Unity subscribers with additional caller information before message playback, consider the following requirements:

- Subscribers hear sender information before Cisco Unity plays each message only if their accounts are configured to play it. Either a Cisco Unity administrator or a subscriber can specify message playback preferences. (Cisco Unity administrators specify whether subscribers hear sender information before message playback on the Conversation pages in the Cisco Unity Administrator, while subscribers can specify their own message playback preferences in the Cisco Unity Assistant.)
- In addition, to allow Cisco Unity to provide the phone number (ANI or caller ID) information on unidentified callers, your phone system must support sending such information to Cisco Unity. (Refer to your phone system documentation for more information.) When Cisco Unity receives ANI information on a caller, it will make use of only the valid numbers, and ignores any other characters that the phone system sends.

See Bulk Edit Help for details on using it to modify existing subscriber accounts. You use one or both of the following fields on the Conversation tab in Bulk Edit to offer subscribers additional caller information before message playback:

Announce Sender's Extension for Messages from Subscribers	Specifies whether Cisco Unity provides subscribers with additional caller information on subscribers (and call handlers) who leave messages for them.
Announce ANI for Messages from Unidentified Callers	Specifies whether Cisco Unity provides subscribers with additional caller information on unidentified callers who leave messages for them.

Playing New Messages Automatically

By default, subscribers hear the Main menu after they log on to Cisco Unity. You can customize the conversation so that Cisco Unity plays new messages instead. When you do, subscribers no longer have to press a key to play new messages ("Press 1 for new messages") because Cisco Unity begins playing them automatically.

Otherwise, the conversation that subscribers hear sounds and acts the same:

- Cisco Unity plays the subscriber recorded name, alternate greeting notification, new message counts, and the Message Type menu as specified.
- System broadcast messages, full mailbox warnings, reminders to reset passwords, and other such prompts are likewise played before Cisco Unity begins playing new messages.
- Subscribers must indicate whether they want to save or delete the message before Cisco Unity plays the next new message.
- Subscribers can exit message playback to hear the Main menu at any time.

If subscribers have no new messages, the Main menu is played as usual.

To specify that Cisco Unity plays new messages automatically in a template or for an individual subscriber, do the following procedure. (To make the change for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.)

To Specify That Cisco Unity Plays New Messages Automatically

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **New Messages Automatically** check box.

Step 3 Click the **Save** icon.fs

Pressing ## or 00 to Switch Search Modes

When subscribers use Cisco Unity to address messages, edit private lists, or find messages by phone, they search for a subscriber either by spelling the name or by entering the extension. Subscribers can switch search modes by pressing ## or 00. By default, Cisco Unity responds to either key combination; you do not need to configure it to do so.

It is important to note, however, that when subscribers press 00 to switch search modes, they will experience a delay before Cisco Unity responds. To avoid the delay, subscribers can press ## rather than press 00. Alternatively, you can reduce the amount of time that Cisco Unity waits for key presses so that subscribers no longer experience the delay when pressing 00.

Reducing the amount of time that Cisco Unity waits for more key presses can eliminate the delay when subscribers press 00 to switch search modes, but at the same time, it also reduces the time that Cisco Unity waits for additional key presses as subscribers address messages, update passwords, change call transfer or message notification numbers, and so on. For this reason, we recommend that you reduce the value specified for the The Wait <x> Milliseconds for Additional Key Presses When Entering Names and Numbers field only for individual subscribers who are likely to use 00, rather than for all subscribers who are associated with a Cisco Unity server.

The Wait <x> Milliseconds for Additional Key Presses When Entering Names and Numbers field is on the Conversation pages for individual subscribers in the Cisco Unity Administrator. By default, Cisco Unity waits 3,000 milliseconds for additional key presses when entering names and numbers.

Prompting Subscribers to Confirm Addressees by Name

By default, when subscribers send, forward, or reply to messages by phone, Cisco Unity does not ask them to confirm each addressee that they add—even when they address a message by entering subscriber extensions. For subscribers who prefer that Cisco Unity confirm each addressee by name (regardless of how they add the addressee), you can specify that Cisco Unity will announce "<subscriber name> added" after each addressee is added.

To specify that Cisco Unity will prompt subscribers to confirm addressees by name, do the following "To Specify That Cisco Unity Will Prompt Subscribers to Confirm Addressees by Name" procedure for an individual subscriber or in a subscriber template. (To make the change for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.)

To Specify That Cisco Unity Will Prompt Subscribers to Confirm Addressees by Name

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **Confirm Addressee by Name** check box.

Step 3 Click the **Save** icon.

Prompting Subscribers to Continue Addressing

By default, when subscribers address messages by phone ("Press 2 to send" or when forwarding a message), Cisco Unity allows them to add a single recipient and then prompts them to indicate what they want to do next ("To add another recipient, press 1. For message options, press 3. To record, press #."). Subscribers who send and forward messages to multiple recipients may find pressing 1 to continue addressing after each recipient tedious and time-consuming. If this is an issue for subscribers in your organization, you can specify that Cisco Unity will instead allow subscribers to continue adding names after each recipient. In this way, you can streamline the addressing process when subscribers send and forward messages to multiple recipients, which may be a welcome change for those who routinely send messages to more than one recipient.

However, if you make the change, consider that when subscribers address messages to single recipients, they are now required to press an additional key to send a message in the following situations:

- When subscribers forward messages to single recipients rather than multiple recipients, they will be required to press one additional key.
- When subscribers send messages to single recipients and Cisco Unity is set up to prompt them to record messages before addressing them, they will be required to press one additional key.

To specify that Cisco Unity prompts subscribers to continue addressing, do the following "To Specify That Cisco Unity Prompts Subscribers to Continue Addressing" procedure for an individual subscriber or in a subscriber template. (To make the change for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.) Note that the Cisco Unity conversation offer a way for subscribers to make the change themselves.

Continuous (or "streamlined") addressing is available for use with all conversations and send menu styles.

Note Specifying that Cisco Unity prompts subscribers to continue addressing does not affect the order in which Cisco Unity prompts subscribers to address and record when they send or forward messages to other subscribers.

To Specify That Cisco Unity Prompts Subscribers to Continue Addressing

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **Continue Adding Names After Each Addressee** check box.

Step 3 Click the **Save** icon.

Specifying the Amount of Time to Skip Back or Ahead When Rewinding or Fast-Forwarding Messages

By default, when subscribers are listening to messages, when they rewind or fast-forward the message, Cisco Unity skips back or ahead in the message by five seconds.

You can also change this setting by using the Bulk Edit utility, and subscribers can enable and adjust the settings themselves on the Phone Menu Preferences page in the Cisco Unity Assistant.

To Change the Amount of Time to Skip Back or Ahead When Rewinding or Fast-Forwarding Messages

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Change the value of the **Fast-Forward Messages By** and the **Rewind Messages By** fields, depending on the desired behavior.

Step 3 Click the **Save** icon.

Specifying the Conversation Styles Offered in the Cisco Unity Assistant

You can specify the conversation styles that are offered to subscribers in the Cisco Unity Assistant. For example, you may want subscribers to choose among only the standard, Optional 1, and Alternate Keypad Mapping N conversations.

To Specify the Conversation Styles Offered in the Cisco Unity Assistant

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 In the **Conversation Styles Offered in Cisco Unity Assistant** section, check the conversation style that you would like to be offered to subscribers in the Cisco Unity Assistant.

If you do not select any conversation style to be offered in the Cisco Unity Assistant, subscribers will see only the conversation style that you have assigned to them in the Cisco Unity Administrator.

Step 3 Click the **Save** icon.

Specifying How Cisco Unity Behaves When Subscribers Have Their Alternate Greeting Enabled

Because an alternate greeting overrides all other greetings, subscribers can use it 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....”) Subscribers can use either the Cisco Unity phone menus or the Cisco Unity Assistant to record their alternate greeting and to specify how long they want it enabled.

For as long as an alternate greeting is enabled, you can specify that Cisco Unity:

- Plays a prompt to notify subscribers when their alternate greeting is enabled. Cisco Unity plays the prompt immediately after subscribers log on to Cisco Unity by phone, and then Cisco Unity plays a menu from which subscribers can choose to leave their alternate greeting on, turn it off, or play it. (The Cisco PCA automatically displays a reminder when subscribers have their alternate greeting turned on, and indicates which caller options you enabled for them.) To customize Cisco Unity so that it plays a prompt letting subscribers know that their alternate greeting is enabled, do the “To Enable the Alternate Greeting Notification Prompt” procedure on page 17-17.
- Transfers callers to the greeting without ringing the subscriber phone when the calls are transferred from the automated attendant or a directory handler to the subscriber extension. (The subscriber phone will still ring if an outside caller or another subscriber dials a subscriber extension directly.) This option is particularly well-received by subscribers who share a phone. To specify whether Cisco Unity transfers callers directly to the alternate greeting without ringing the subscriber phone,

prevents them from skipping the greeting, and/or prevents callers from leaving messages, do the "To Specify Caller Options for Alternate Greetings" procedure on page 17-17. (If you want to enable the caller options for a group of subscribers, you can use the Bulk Edit tool available in Tools Depot.)

- Prevents all callers from skipping the greeting. In this way, you can increase awareness of a subscriber absence for callers who hear the greeting after dialing the subscriber extension or being transferred to the subscriber greeting from a call handler.
- Prevents callers from leaving messages. While preventing callers from leaving messages does not prevent other subscribers from sending, replying to, and forwarding messages to someone who has the alternate greeting enabled, it can help reduce the number of messages received in a subscriber mailbox when the subscriber is out of the office and does not plan to check messages regularly.
- To set up the Cisco Unity server to send a notice to subscribers when they leave, send to, reply to, or forward messages to other subscribers who have their alternate greeting enabled, do the "To Enable Alternate Greeting Notices for a Cisco Unity Server (Voice Messaging Only)" procedure on page 17-18.

  Due to conflicts with the "Out of Office" rule in Outlook, enabling alternate greeting notices for Unified Messaging systems is not supported.

To Enable the Alternate Greeting Notification Prompt

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Check the **Alternate Greeting Notification** check box.

The check box controls only whether subscribers are notified that their alternate greeting is enabled when they access Cisco Unity by phone; subscribers are always notified when their alternate greeting is enabled in the Cisco PCA, even when this box is unchecked.

Step 3 Click the **Save** icon.

To Specify Caller Options for Alternate Greetings

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Greetings** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Greetings** page.

Step 2 Check any or all of the following check boxes to indicate how you want Cisco Unity to handle calls to subscribers who have their alternate greetings enabled:

- **Transfer Callers to Greeting Without Ringing the Subscriber Phone**
- **Prevent Callers From Skipping the Subscriber Greeting**
- **Prevent Callers From Leaving Messages**

Note The Transfer Callers to Greeting Without Ringing the Subscriber Phone setting only works when calls are transferred from the automated attendant or a directory handler to the subscriber extension; the setting does not apply when an outside caller or another subscriber dials a subscriber extension directly.

Step 3 Click the **Save** icon.

To Enable Alternate Greeting Notices for a Cisco Unity Server (Voice Messaging Only)

Enabling alternate greeting notices can only be done per server. In digitally networked environments, the feature should be enabled for all Cisco Unity servers in the network.

After you do the following procedure, when subscribers associated with the Cisco Unity server enable their alternate greeting, Cisco Unity will send an alternate greeting notice to any subscriber who sends a message to them. (Cisco Unity will not send notices in response to messages sent to subscribers who already had their alternate greeting enabled before notices were turned on.) If you later choose to disable alternate greeting notices, any existing notices in subscriber mailboxes are no longer available to subscribers until you enable the feature again and subscribers will no longer receive notices—even if other Cisco Unity servers in the network have the feature enabled.

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Conversation—Alternate Greeting Notices**.

Step 4 In the New Value list, click **1** and click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Restart the Cisco Unity software.

Note If you do not restart the Cisco Unity software when you enable or disable the feature, notices do not behave as expected.

Step 8 As applicable, repeat the procedure for each Cisco Unity server at your site.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

Specifying the Style of Phone Menus That Subscribers Hear When They Send, Reply to, and Forward Messages

You can specify the menus that subscribers hear when they send, reply to, and forward messages over the phone. The send menu style affects what subscribers hear after they have recorded and addressed a message.

By default, subscribers hear the Streamlined Send menu. Compared to the tiered menus that are offered with the Standard send menu, the Streamlined Send menu is designed so that subscribers use fewer keystrokes to mark messages urgent, request receipts, and perform other tasks after they have addressed and recorded a message.

The following table compares the two send menu styles:

Standard Send Menus	Streamlined Send Menus
# - Send message 1 - Message options 1 - Change address 1 - Add name 2 - Hear all names 3 - Remove name 2 - Change recording 1 - Hear recording 2 - Save recording 3 - Re-record 4 - Add to recording 3 - Set special delivery 1 - Urgent 2 - Return receipt 3 - Private 4 - Future delivery 4 - Review message # - Send message	# - Send message 1 - Urgent 2 - Return receipt 3 - Private 4 - Future delivery* 5 - Review message 6 - Re-record 7 - Add to recording 91 - Add name 92 - Hear all names (and delete names)

Note When subscribers switch from Standard Send menus to Streamline Send menus, they may continue to use old shortcuts to set special delivery options before sending a message. For example, out of habit, subscribers may press 131# to mark a message urgent and send it. In the Streamlined Send menu, using the same shortcut marks the message urgent, private, and then marks the message normal again before it is sent. As a result, the recipient receives a private message, and not the urgent message as the sender intended. As with any conversation change, make sure that subscribers understand the implications of changing from Standard to Streamlined Send menus so that they can adjust their behavior accordingly.

Streamlined Send menus also offer easier navigation of lists when subscribers address messages:

List Navigation with Standard Send Menus	List Navigation with Streamlined Send Menus
Cisco Unity presents six names at a time when subscribers select addressees from a list of names. When subscribers hear the name they want, they select the name by pressing the number (from 1 to 6) that corresponds to the name; if they do not make a selection, Cisco Unity presents the next set of six names.	Cisco Unity offers a "skip and scan" method of selecting names from lists. Cisco Unity presents the entire list of matches, and when subscribers hear the name they want, they press # to select it. (Subscribers press 3 to delete a name when reviewing lists.) They can also press 7 or 9 to skip to, respectively, the previous or next name in the list, and can press 7-7 or 9-9 to skip to the beginning or end of the list. In this way, subscribers can navigate and select names from long lists more quickly and efficiently, which may reduce the time that they spend addressing messages.

Note The send menu style that you select does not affect the order in which Cisco Unity prompts subscribers to address and record when they send or forward messages to other subscribers, nor does it affect whether Cisco Unity prompts subscribers to continue addressing.

Do the following "To Specify a Send Menu Style" procedure to specify the send menu style on the applicable Conversation page for a subscriber template or an individual subscriber in the Cisco Unity Administrator. To make the change for a group of subscribers, use the Bulk Edit tool available in Tools Depot. Alternatively, subscribers can specify the send menu style that they want to hear on the Advanced Settings page in the Cisco Unity Assistant.

To Specify a Send Menu Style

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 From the Send Message Style list, click the style of menu that you want subscribers to hear.

Step 3 Click the **Save** icon.

CHAPTER 18c

Managing Voice-Recognition Features

Voice-recognition features allow subscribers to interact with Cisco Unity by speaking rather than by using the phone keypad. The features are licensed by number of concurrent sessions, and require installation and configuration of voice-recognition software on a separate and dedicated server. Voice recognition is not available to outside callers.

You configure voice recognition settings on the System > Voice Recognition page in the Cisco Unity Administrator.

For information on installing and configuring a separate voice-recognition server, see the applicable Cisco Unity installation guide, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

See the following sections in this chapter for additional details about administering voice-recognition features:

Access to Voice Recognition Features

You enable access to the voice-recognition features on the applicable Conversation page for a subscriber template or an individual subscriber in the Cisco Unity Administrator, or by using the Bulk Edit utility. When voice recognition access is enabled, subscribers can enable and disable the Press-or-Say input style by phone or by using the Cisco Unity Assistant.

Do the following "To Enable Access to Voice-Recognition Features" procedure to enable voice-recognition access for subscribers. When subscribers have voice-recognition access, they can enable and disable the Press-or-Say input style by phone or by using the Cisco Unity Assistant. (See also the "Press-or-Say Phone Input Style" section on page 18-2.)

To Enable Access to Voice-Recognition Features

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.

- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Under Phone Menu Options, click **Allow Access to Voice-Recognition Features** so that it is selected.

Step 3 Click the **Save** icon.

Press-or-Say Phone Input Style

The Press-or-Say phone input style gives subscribers the options of pressing the key or saying the number that corresponds to a menu option.

In addition, when addressing messages, adding names to private lists, and using the Message Locator feature, subscribers can say the names of recipients instead of spelling them by using the phone keypad. To improve the accuracy of name recognition, you can enter alternate spellings for the names of individual subscribers. Alternate spellings are entered on the Alternate Name page for individual subscribers in the Cisco Unity Administrator. See either the "Voice Addressing" section on page 18-2 or the "Managing the Alternate Names List" section on page 18-3 for more information.

You enable the Press-or-Say input style on the applicable Conversation page for a subscriber template or an individual subscriber in the Cisco Unity Administrator, or by using the Bulk Edit utility. Do the following "To Enable the Press-or-Say Input Style" procedure to enable the Press-or-Say input style for subscribers. If voice-recognition features are enabled for subscribers, then subscribers can enable or disable the Press-or-Say input style over the phone or by using the Cisco Unity Assistant.

The Press-or-Say feature requires an additional server running voice-recognition software. For more information, see the "Access to Voice Recognition Features" section on page 18-1.

To Enable the Press-or-Say Input Style

Step 1 In the Cisco Unity Administrator, go to the applicable page:

- To modify the template that you will use to create subscriber accounts, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify. Then browse to the **Conversation** page.
- To modify an existing subscriber account, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Conversation** page.

Step 2 Under Phone Menu Options, verify that the **Allow Access to Voice-Recognition Features** check box is selected.

Step 3 Under Phone Menu Options, click the **Use Press-or-Say Phone Input Style (Includes Voice Addressing)** check box so that it is selected.

Step 4 Click the **Save** icon.

Voice Addressing

Cisco Unity recognizes spoken subscriber names, so subscribers do not have to spell them by saying letters. They can say subscriber names while addressing messages, adding subscribers to private lists, using Message Locator, or addressing public distribution lists.

See the following sections:

- Managing the Alternate Names List, page 18-3
- Updating the Name Grammar Files, page 18-4
- Setting the Search Scope for Improved Voice Name Recognition, page 18-5

For additional information on improving name recognition, see the "Voice-Recognition Considerations" section on page 18-5.

Managing the Alternate Names List

Alternate names are different versions of a subscriber name than what is listed in the corporate directory. Cisco Unity considers these names when a subscriber uses voice recognition to address messages, add subscribers to private lists, use Message Locator, or address public distribution lists.

You create alternate names for individual subscribers, and cannot add or edit alternate names from the subscriber template. Also, it is important to note that any alternate names you create are stored locally and are not propagated to other Cisco Unity servers. Any alternate names that you add or modify are not active until there has been a grammar rebuild. See the "Updating the Name Grammar Files" section on page 18-4 for more information on rebuilding the name grammar files.

When creating alternate names, you might want to add common variants of a name that subscribers might use. For example, you might want to add Bill, Billy, and Will for the name William. Or, you could use this feature to add another version of an uncommon name, unusual nicknames, or maiden names. For example, if a subscriber asked Cisco Unity to address "Mary Jameson," which was the maiden name of Mary Brown, Cisco Unity could reference this information and add the correct subscriber to the message. You could also use alternate names to add phonetic spellings of hard-to-pronounce names. For example, you could add "Goolay" as an alternate name for the last name "Goulet."

Note that name recognition accuracy degrades as the number and variability of names increase. In addition, name recognition tends to be less accurate for non-English names. For this reason, we recommend that you include only the most commonly-known alternate names for subscribers.

See the following procedures:

- To Add Alternate Names, page 18-3
- To Edit Alternate Names, page 18-4

Note that you cannot add or edit alternate names on a subscriber template.

To Add Alternate Names

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page and find the applicable subscriber. Then browse to the **Alternate Names** page.

Step 2 Under Add, in the Alternate Names fields, enter the alternate names.

Step 3 Click **Add**.

Step 4 Repeat Step 2 and Step 3 until all alternate names have been added.

To Edit Alternate Names

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page and find the account that you want to change. Then browse to the **Alternate Names** page.

Step 2 Do any of the following:

- In the Alternate Names fields, enter changes to the already-existing alternate names.
- If you want to delete an alternate name, check the check box next to the name.

Step 3 Click the **Save** icon.

Updating the Name Grammar Files

The name grammar files should be updated immediately after Cisco Unity installation and configuration, and updated routinely anytime Cisco Unity subscribers are created, added or imported to the Cisco Unity directory. The names of new Cisco Unity subscribers and their alternate names will not be immediately available to the voice-recognition system unless the grammar files are updated.

By default, the name grammar files are scheduled to update automatically at 1:00 a.m. daily. To make changes available immediately or at a different scheduled time, do one of the following procedures:

- To Schedule When Cisco Unity Automatically Rebuilds the Name Grammar Files, page 18-4
- To Manually Rebuild the Name Grammar Files, page 18-4

Note Depending on the size of the directory, name grammars may take a long time to build and may affect system performance. We recommend that you schedule the automatic rebuild to occur at off-peak times. By default, the automatic rebuild starts at 1:00 a.m. Manual updates are recommended only when troubleshooting or during the initial Cisco Unity configuration.

To Schedule When Cisco Unity Automatically Rebuilds the Name Grammar Files

Step 1 In the Cisco Unity Administrator, go to the **System > Voice Recognition > Settings** page.

Step 2 Under Grammar Engine, in the **Automatic Rebuild Time** fields, enter the new time.

By default, the automatic rebuild starts at 1:00 a.m. We recommend that you schedule the automatic rebuild to occur at off-peak times.

Step 3 Click the **Save** icon.

To Manually Rebuild the Name Grammar Files

Depending on the size of the directory, name grammars may take a long time to build and may affect system performance. Manual updates are recommended only when troubleshooting or during the initial Cisco Unity configuration.

Step 1 In the Cisco Unity Administrator, go to the **System > Voice Recognition > Settings** page.

Step 2 Under Grammar Engine, click **Start**.

Setting the Search Scope for Improved Voice Name Recognition

You can set the default search scope to be used for looking up names when subscribers are addressing messages using voice recognition. This setting is only used if the subscriber who is addressing the message does not have the addressing search scope limited to a directory handler on the Subscriber > Profile page.

Cisco Unity deployments can scale to very large systems with tens of thousands of users across networked servers. Name recognition accuracy degrades as the number and variability of names increase. In addition, name recognition tends to be less accurate for non-English names. Depending on the number of names in your Cisco Unity subscriber global directory, you may want to limit searches to reduce the number of names processed by the voice-recognition server.

Note that the number of names is not always equal to the number of subscribers and distribution lists in a scope. The number of names also includes alternate spellings of each name. For example, a 100 user company that has one alternate name for each subscriber would generate a global directory scope with 200 names. For this reason, it would be advisable to include only the most common alternate names when considering alternate names.

To Set the Search Scope for Improved Name Recognition

Step 1 In the Cisco Unity Administrator, go to the **System Settings > Voice Recognition > Settings** page.

Step 2 Under Voice Recognition Server, select one of the following options from the **Limit Searches to The** list:

- **Local Server**—All local subscribers and public distribution lists on the Cisco Unity server handling the call. This scope is expected to have better accuracy than global directory or dialing domain.
- **Dialing Domain**—All local and remote subscribers and public distribution lists that are in the local dialing domain. This scope is expected to be smaller than the global directory, but could still be fairly large. It should have better accuracy than the global directory.
- **Global Directory**—All local subscribers and public distribution lists, all named remote subscribers and remote public distribution lists. This will be the largest search scope and may have the worst accuracy of all the search scopes.

Step 3 Click the **Save** icon.

Voice-Recognition Considerations

See the following sections:

- General Considerations, page 18-6
- Improving Voice Recognition Performance, page 18-6

General Considerations

You may want to tell subscribers about the following general considerations when they use the Press-or-Say phone input style. See the *Cisco Unity User Guide* for additional voice-recognition usage considerations.

- When voice recognition is available on the system, you will hear "Voice recognition on" after logging on to Cisco Unity. If voice recognition is unavailable, you do not hear the prompt and cannot use the Press-or-Say input style for the duration of the call. You may be able to use the input style if you hang up and try again in a few moments.
- Do not say the names of menu options. Instead, you should say the key for the menu options you want. (For example, when Cisco Unity prompts you to press 1 to play new messages, do not say "Play new messages." Instead, say "One." (Or you can press the 1 key.) Where appropriate, you can also say "pound" and "star."
- After you say your entry, you must pause to allow Cisco Unity to detect that you are done with the entry. Because of the pause, the system may seem slower when you say options than when you press keys for options.
- When entering multi-digit numbers, you must say each digit individually. For example, to enter extension 3200, say "Three-two-zero-zero." Cisco Unity does not recognize "Thirty-two hundred" or "Three thousand, two hundred." For long extensions or phone numbers, you can say the entire number before pausing, but you must say each digit in the number.
- You cannot say multi-digit shortcuts to jump ahead in the menus. For example, you cannot say "Four-one-two" to turn on the alternate greeting. Instead, you must say the single key number for the first menu option, then pause for the system to recognize your entry before you say the key number for the option in the next menu. (You can enter menu shortcuts by pressing keys.)
- It is possible to press keys and to say key numbers for any menu option. For example, you could choose an option from one menu by pressing a key, then choose an option from the next menu by saying the number. However, if you press the key and say the number for a single option, the key press takes precedence over the spoken information. For example, if you say "One-pound," then press "4-#" while entering a month, Cisco Unity will recognize April as the month selected rather than January.

Improving Voice Recognition Performance

- Subscribers may find that voice recognition is less accurate when used in conditions where there is background noise—for example, if a subscriber is using a speaker phone or a mobile phone. In these situations, subscribers can either use key presses to enter commands or turn off the Press-or-Say feature for the duration of the call. For information on how to disable the Press-or-Say feature, see the "Press-or-Say Phone Input Style" section on page 18-2.
- If a subscriber voice name is frequently not recognized, consider using alternate names to add phonetic spellings of hard-to-pronounce names. For example, you could add "Goolay" as an alternate name for the last name "Goulet." For information on managing alternate names, see the "Managing the Alternate Names List" section on page 18-3.
- Performance issues may be indicated by frequent time-outs, if the voice recognition system is slow to respond, or if there are consistent problems in understanding how a name is pronounced. Depending on the size of your global directory, you may want to limit searches to reduce the number of names processed by the voice-recognition server. See the "Setting the Search Scope for Improved Voice Name Recognition" section on page 18-5.

CHAPTER 19

Managing Classes of Service

See the following sections in this chapter:

Class of Service Settings Overview

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

- Controls access to the Cisco Unity Administrator and to features, such as Text to Speech e-mail or live reply.
- Controls how subscribers interact with Cisco Unity. For example, a COS dictates the maximum length of subscriber messages and greetings, whether subscribers can choose to be listed in directory assistance, and whether subscribers can send messages to a public distribution list.
- Specifies the restriction table used to control the phone numbers subscribers can use for fax delivery, message notification, call transfer, and other tasks.

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

Predefined Classes of Service

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

{Default Subscriber}	Contains settings that are applicable to subscribers. By default, this COS is associated with the {Default Subscriber} template.
{Default Administrator}	Contains settings that are applicable to Cisco Unity Administrators. By default, this COS is associated with the {Default Administrator} template, and has all of the settings checked on the Subscribers > Class of Service > System Access Page.
Hotel Guest	When the Cisco Unity Hospitality and Property Management System Integration is installed, this class of service contains settings that are applicable to Cisco Unity hotel guest subscribers. By default, this COS is associated with the Hotel Guest template.

How a Class of Service Works

A COS is specified in each subscriber template, and controls what subscribers can do in Cisco Unity. This means that when a subscriber wants to update call transfer settings, for example, the COS that is associated with the subscriber account determines whether the subscriber can make the change. This is true whether the subscriber is logged on to Cisco Unity by phone, or is using the Cisco Unity Assistant.

On the other hand, when an administrator uses the Cisco Unity Administrator to change settings for the subscriber, Cisco Unity does not consider the limitations set by the subscriber COS. Instead, Cisco Unity considers the limitations set by the administrator COS before permitting the change. This allows an administrator, when necessary, to override the limitations of the COS of a particular subscriber.

Creating, Modifying, Assigning, and Deleting Classes of Service

You can modify the predefined classes of service, and you can create new ones by using the following procedures. 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 subscriber Cisco Unity accounts; however, a subscriber 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 subscribers to the COS only if enough licenses are available.

See the following procedures:

- To Create a New Class of Service, page 19-2
- To Modify a Class of Service, page 19-2
- To Assign or Reassign Subscribers to a Class of Service, page 19-3
- To Delete a Class of Service, page 19-3

To Create a New Class of Service

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Class of Service dialog box, enter information as applicable in the Name field.

Step 4 Select **New Class of Service** or **Based on Existing Class of Service**. If you select Based on Existing Class of Service, select the applicable class of service in the Based On field.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new class of service, and then click the **Save** icon.

To Modify a Class of Service

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the COS that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

To Assign or Reassign Subscribers to a Class of Service

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the name of the class of service to which subscribers are currently assigned.

Step 4 Go to the **Subscribers > Class of Service > Subscribers** page.

Step 5 Click **Assign** or **Reassign**, as applicable.

Step 6 Enter the name of a subscriber. You also can enter ***** for a list of all subscribers, or enter one or more characters followed by * to narrow your search.

Step 7 Click **Find**.

Step 8 From the list provided, select the names of the subscribers to be assigned or reassigned. To select more than one name, hold down the Ctrl or Shift key.

Step 9 Do one of the following actions, as applicable:

- Click the **Assign** button.
- Select the applicable class of service, and then click the **Reassign** button.

To Delete a Class of Service

Note You cannot delete a COS that has subscribers assigned to it without first reassigning the subscribers to another COS. See the "To Assign or Reassign Subscribers to a Class of Service" procedure on page 19-3.

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Class of Service** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the COS that you want to delete.

Step 4 Click the **Delete** icon. Confirm the deletion by clicking **Delete** again.

CHAPTER 20

Managing Subscriber Templates

See the following sections in this chapter:

Subscriber Template Overview

When you create subscriber accounts in Cisco Unity, you can base each account on a subscriber template. Subscriber templates contain settings that are applicable for most subscribers of a particular type (such as a department).

Basing new subscriber accounts on a template minimizes the number of settings that must be modified on individual subscriber accounts, making the job of creating subscribers easier. It is important to note that 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. See the "Modifying Subscriber Accounts" section on page 21-29 for information on modifying subscriber accounts after they have been created.

Predefined Templates

Cisco Unity comes with the following predefined subscriber templates:

- {Default Subscriber} Template—The settings on this template are suitable for most subscribers.
- {Default Administrator} Template—The Class of Service setting on this template assigns subscribers to the {Default Administrator} class of service, which gives subscribers access to the Cisco Unity Administrator.
- {Default Bridge Subscriber} Template—The settings on this template are suitable for Cisco Unity Bridge subscribers. For more information about Bridge subscribers, see the applicable *Networking Guide for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- {Default Hotel Guest} Template—If you have installed the Cisco Unity Hospitality and Property Management System integration, the settings on this template are suitable for Cisco Unity Hotel Guest subscribers. The Class of Service setting on this template assigns subscribers to the Hotel Guest class of service.

Creating and Modifying Subscriber Templates

You can modify the predefined templates, but you cannot delete them. You can also create an unlimited number of additional templates.

To Create a New Template

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Template** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Subscriber Template dialog box, enter a name.

Step 4 Select **New Template** or **Based on Existing Template**. If you select Based on Existing Template, select the applicable template in the Based On field.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new template, and then click the **Save** icon.

To Modify a Template

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Template** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the template that you want to modify.

Step 4 Change settings as applicable, and then click the **Save** icon.

CHAPTER 21

Managing Subscriber Accounts

Creating Subscriber Accounts Overview

Anyone who has an account on Cisco Unity is a subscriber. You create regular and external (AMIS, Bridge, Internet, or VPIM) subscriber accounts by using either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator.

If you are planning to create subscriber accounts for administrators to use when accessing the Cisco Unity Administrator, first review the "About the Accounts That Can Be Used to Administer Cisco Unity" section on page 2-1, and then return to this chapter.

Creating Regular Subscriber Accounts

See the following sections in this chapter:

- Issues to Consider Before Creating Regular Subscriber Accounts, page 21-2—Describes the issues that you must consider before creating subscriber accounts.
- Site-Specific Issues to Consider, page 21-5—Contains topics on how Cisco Unity handles Active Directory accounts, considerations for securing passwords, where Cisco Unity stores subscriber account information, and more.
- Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts, page 21-9—Provides basic information about using the Cisco Unity Bulk Import wizard to create regular subscriber accounts, either by importing user data into Cisco Unity from Active Directory or from a CSV file.
- Using the Cisco Unity Administrator to Create Individual Subscriber Accounts, page 21-25—Provides information about using the Cisco Unity Administrator to create a regular subscriber account by adding a new user to Active Directory or by importing existing user data from Exchange.
- Using Integrated Mailbox Configuration to Create Individual Subscriber Accounts, page 21-27 *(For integrations with Cisco Unified Communications Manager only)*—Provides information about using the Integrated Mailbox Configuration to create individual Cisco Unity subscriber accounts.
- Issues to Consider After Creating Subscriber Accounts, page 21-28—Lists the tasks to consider after you have created Cisco Unity subscriber accounts.

After subscriber accounts have been created, review the following sections, as applicable:

- Modifying Subscriber Accounts, page 21-29
- Deleting Subscriber Accounts, page 21-29

Creating External Subscriber Accounts

See the following task lists, as applicable:

- To create AMIS subscriber accounts, see the "Setting Up Cisco Unity to Use AMIS" section in the "AMIS Networking" chapter in the *Networking Guide for Cisco Unity*.
- To create Internet subscriber accounts, see the "Creating Internet Subscriber Accounts" section in the "Internet Subscribes" chapter in the *Networking Guide for Cisco Unity*.
- To create Bridge subscriber accounts, see the "Task List: Setting Up Cisco Unity and the Bridge for Networking" section in the "Setting Up Cisco Unity and the Bridge for Networking" chapter in the *Networking Guide for Cisco Unity Bridge*.
- To create VPIM subscriber accounts, see the "Setting Up Cisco Unity to Use VPIM Networking" section in the "VPIM Networking" chapter in the *Networking Guide for Cisco Unity*.

The guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Issues to Consider Before Creating Regular Subscriber Accounts

This section lists—in order—the issues that you must consider before creating subscriber accounts. If you are creating subscriber accounts that you want to use to administer Cisco Unity, you should review the "About the Accounts That Can Be Used to Administer Cisco Unity" section on page 2-1 in addition to the information that follows.

1. **Cisco Unity Configuration and Permissions**

If you are unsure whether the account that you are using has sufficient rights and permissions to create subscriber accounts, or whether Cisco Unity is properly configured to work with your message store, use the following procedure to run the SysCheck diagnostic tool.

To Check Cisco Unity Setup and Permissions by Using the Cisco Unity SysCheck Tool

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **SysCheck**.

Step 3 On the Welcome to the Cisco Unity Configuration Wizard page, click **Select Configuration Tests**, and click **Next**.

Step 4 Uncheck the boxes for the message stores that are not connected to Cisco Unity.

Step 5 Click **Test**.

Step 6 In the Test Results box, click the link provided to view the test results.

Step 7 If no errors are reported, proceed to Step 8. Otherwise, do the following sub-steps:

a. Follow the advice offered in the Resolution column to correct each configuration or permissions error.

b. Return to the Completing the Check Unity Configuration Wizard page, and click **Finish**.

c. Repeat Step 2 through Step 7 until no errors are reported.

Step 8 Click **Finish**.

2. **Licenses**

Confirm that you have the Cisco Unity user licenses that are required for the type of subscriber accounts that you plan to create. You can view the number of licenses purchased, and the number that are used and unused on your system, from the System > Licensing page in the Cisco Unity Administrator. If you need additional licenses, contact your reseller. If you need to upgrade your licenses, see the "Adding Cisco Unity User Licenses" section in the "Adding Features to the Cisco Unity System" chapter of the *Reconfiguration and Upgrade Guide for Cisco Unity*. (The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)

3. **Account Policies**

Account policies govern subscriber passwords and account lockouts for all Cisco Unity subscriber accounts. There are two account policies that you can set up to secure how subscribers access Cisco Unity:

- See the "Managing Account Policy Settings" chapter to set up system-wide phone password and lockout policies that apply to phone access.
- See the "Authentication for Cisco Unity Applications" chapter of the *Security Guide for Cisco Unity* for information on setting up system-wide logon, password, and lockout policies that apply when subscribers access the Cisco Unity Administrator (if it is configured to use Anonymous authentication) and the Cisco Personal Communications Assistant (PCA). The *Security Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Each account policy has default settings that you can modify in the Cisco Unity Administrator.

4. **Enhanced Phone Security**

You can set up Cisco Unity subscriber accounts to use a secure logon method when subscribers access Cisco Unity by phone. See the "Determining Whether to Offer Enhanced Phone Security" section in the "Authentication for Cisco Unity Applications" chapter of the *Security Guide for Cisco Unity* for information on enhanced phone security, if desired. If you choose to set up enhanced phone security, then you must also create a new class of service or modify an existing one for the subscribers who will be using enhanced phone security (see the next task). (The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)

5. **Classes of Service**

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

- Controls access to the Cisco Unity Administrator and to features such as Text to Speech e-mail.
- Controls how subscribers interact with Cisco Unity. For example, a COS dictates the maximum length of subscriber messages and greetings, whether subscribers can choose to be listed in directory assistance, whether subscribers use a secure logon method to access Cisco Unity by phone, and whether subscribers can send messages to a public distribution list.
- Specifies the restriction table used to control the phone numbers that subscribers can use for fax delivery, message notification, call transfer, and other tasks.

In the Cisco Unity Administrator, a COS is specified in each subscriber template; thus, a subscriber is assigned to the COS that is specified in the template on which the subscriber account is based. Cisco Unity includes predefined classes of service, which you can modify. You can also create new classes of service. For details, see the "Managing Classes of Service" chapter.

6. **Restriction Tables**

Restriction tables in the Cisco Unity Administrator allow you to control the phone numbers that subscribers and administrators can use for:

- Transferring calls
- Recording and playback by phone from Cisco Unity applications, when the phone is the designated recording and playback device in the Media Master (the Media Master is available in the Cisco Unity Administrator, the Cisco Unity Assistant, the Cisco Unity Inbox, and ViewMail).
- Delivering faxes to a fax machine
- Sending message notifications
- Sending AMIS messages
- System transfers

Each class of service specifies a restriction table for call transfers, one for message notification, and one for fax deliveries. Cisco Unity comes with predefined restriction tables, which you can modify. See the "Managing Restriction Tables" chapter for details.

7. **Public Distribution Lists**

Public distribution lists are used to send voice messages to multiple subscribers at the same time. Cisco Unity assigns new subscribers to the public distribution lists that are specified in the template on which the subscriber account is based. The class of service associated with a subscriber account dictates whether that subscriber can use Cisco Unity to send messages to public distribution lists. See the "Managing Distribution Lists" chapter for details.

8. **Subscriber Templates**

In the Cisco Unity Administrator, you can specify settings for a group of subscribers by using a subscriber template. The settings from the template you choose are applied to all subscriber accounts as the accounts are created. See the "Managing Subscriber Templates" for details.

9. **Change the Locale ID of the MAPI Profile for the Cisco Unity Server**

If either of the following statements is true, use the Advanced Settings tool to change a registry key so that the Locale ID of the MAPI profile for the Cisco Unity server matches the language that subscribers use locally:

- You are planning to create new user mailboxes at the same time that you create Cisco Unity subscriber accounts. (This option is available in the Cisco Unity Administrator and in the Cisco Unity Bulk Import wizard.)
- Mailboxes already exist, but users will not have used Microsoft Outlook (or another MAPI client) to access their mailboxes by the time that you create Cisco Unity subscriber accounts for them.

Typically, local language settings for a MAPI client determine the language in which a program such as Microsoft Outlook displays the names for the Inbox, Sent Items, and other message folders. However, under the circumstances described above, the folder names do not appear in the language specified locally, but appear in the language specified by the Locale ID setting of the MAPI profile for the Cisco Unity server instead.

For details on setting up this functionality to avoid this problem, see Advanced Settings tool Help. The setting is called Messaging—Set the Locale ID of the MAPI Profile. Consider creating subscribers in batches according to the language setting that they will use in their MAPI clients. Then change the registry setting as applicable before creating each group of subscribers.

10. **Subscriber Mailboxes Homed in Exchange 2007**

If mailboxes for Cisco Unity subscribers will be homed in Exchange 2007, you must create Active Directory accounts and Exchange mailboxes before you create subscriber accounts. This is true for all methods of creating subscriber accounts.

11. **Bridge Networking Option**

If your installation includes the Bridge Networking option, confirm that the following tasks have been completed so that Cisco Unity subscribers will be able to send messages to and receive messages from subscribers on the Octel servers with which Cisco Unity communicates:

- The Active Directory schema has been extended as required for networking with the Cisco Unity Bridge.
- On the Configuration > Settings page in the Cisco Unity Administrator, the Display Fields Required for Cisco Unity Bridge Networking on Subscribers Profile Page check box has been checked.

12. **Site-Specific Issues**

Review the "Site-Specific Issues to Consider" section on page 21-5. Information presented in the section may affect the tools, tasks, and methods that you use to create subscriber accounts.

Site-Specific Issues to Consider

This section contains several topics that may be important considerations for your particular site. Information presented in these topics may affect the tools, tasks, and methods you use to create subscriber accounts. Review the following sections, as applicable:

How Cisco Unity Handles Active Directory Accounts for the Subscriber Accounts That You Create

Each regular Cisco Unity subscriber account is associated with an Active Directory domain account and an Exchange mailbox in which Cisco Unity stores voice messages. When you create Cisco Unity subscribers using the Cisco Unity Administrator or by importing a CSV file using the Cisco Unity Bulk Import wizard, Cisco Unity can optionally create the associated Active Directory account for each subscriber. (If mailboxes for Cisco Unity subscribers will be homed in Exchange 2007, you do not have this option. You must create Active Directory accounts and Exchange mailboxes before you create Cisco Unity subscriber accounts.) If you let Cisco Unity automatically create Active Directory accounts, the password on the Active Directory accounts is the same for every Cisco Unity subscriber account that was created using the same Cisco Unity template. A subscriber who knows another subscriber's alias and the Active Directory password in the template could access messages for the other subscriber using the Cisco Unity Inbox or an e-mail client, impersonate the user through the Cisco Unity Inbox, or change settings for the other subscriber using Cisco Personal Communications Assistant.

If Cisco Unity is configured for Unified Messaging, the Active Directory accounts must be enabled because they are required for authentication.

If all of the following are true, we recommend that you disable the Active Directory accounts associated with Cisco Unity subscribers:

- Cisco Unity is configured for Voice Messaging.
- Subscribers will only access voice messages using the telephone.

- Subscribers will not access Cisco Personal Communications Assistant or the Cisco Unity Administrator.

Caution If you need Active Directory accounts to be enabled and you are creating the accounts automatically when you create Cisco Unity subscribers, see the "Ensuring That Subscribers Are Assigned Unique and Secure Active Directory Passwords" section on page 21-7.

If you use either the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create subscriber accounts and the associated Active Directory accounts, and you want the Active Directory accounts to be disabled, do the following procedure before you create Cisco Unity subscribers.

To Create Disabled Active Directory Accounts When You Create Cisco Unity Subscribers

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane of Tools Depot, expand Administrative Tools, and double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings list of the Advanced Settings Tool, click **Administration - Disable AD accounts Created by Unity**.

Step 4 In the New Value list, click **1**, and then click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Close Tools Depot.

Ensuring That Subscribers Are Assigned Unique and Secure Phone Passwords

To help protect Cisco Unity from unauthorized access and toll fraud, every subscriber should be assigned a unique phone password. Additionally, each password should be eight or more characters long and non-trivial.

Simply changing the phone password on the Subscribers > Subscriber Template > Passwords page in the Cisco Unity Administrator before you create subscriber accounts does not ensure that subscribers are assigned unique passwords. This is because the template might not be used to assign passwords, and when it is used, each subscriber account that you create is assigned the same password.

Consider the following options to ensure that each subscriber is assigned a unique and secure password at the time that you create the account, or immediately thereafter.

Assigning Unique and Secure Phone Passwords When You Create Subscriber Accounts

Use one of the following methods to assign a unique and secure phone password to each subscriber account that you create:

- Use the Cisco Unity Bulk Import wizard to import user data contained in a CSV file. Include the optional column header DTMF_PASSWORD in the CSV file to overwrite the template password for each subscriber.
- Use the Cisco Unity Administrator to add a subscriber one at a time. Use a different template for each subscriber that you create, specifying a unique and secure phone password in each template. Alternatively, you can use one template for all subscribers, but specify a unique and secure password

before each subscriber account that you add. To avoid recording and distributing the passwords, tell subscribers to use the Cisco Unity Assistant to change their initial phone passwords. (The Cisco Unity Assistant does not require that subscribers enter the old phone password to change it.)

Assigning Unique and Secure Phone Passwords After Creating Subscriber Accounts

After you have created subscriber accounts by using either the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard, use the Cisco Unity Bulk Import wizard to assign a unique phone password to each subscriber account that you created. To avoid recording and distributing the passwords, tell subscribers to use the Cisco Unity Assistant to change their initial phone passwords. (The Cisco Unity Assistant does not require that subscribers enter the old phone password to change it.)

Ensuring That Subscribers Are Assigned Unique and Secure Active Directory Passwords

Subscribers use an Active Directory password to access the Cisco Unity Administrator (when it is configured to use Anonymous authentication) and the Cisco PCA. To protect Cisco Unity from unauthorized access, each subscriber should be assigned a unique Active Directory password. Additionally, each password should be eight or more characters long and non-trivial.

Simply changing the Active Directory password on the Subscribers > Subscriber Template > Passwords page in the Cisco Unity Administrator before you create subscriber accounts does not ensure that subscribers are assigned unique passwords. This is because the template might not be used to assign passwords, and when it is used, each subscriber account that you create will be assigned the same password.

Consider the following options to ensure that each subscriber is assigned a unique and secure password at the time that you create the account, or immediately thereafter.

Assigning Unique and Secure Active Directory Passwords When You Create Subscriber Accounts

Use one of the following methods to assign a unique and secure Active Directory password to each subscriber account that you create:

- Do not use the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create new Active Directory accounts. Instead, first create an Active Directory account for each subscriber by using Active Directory Users and Computers, and assign each user a unique and secure password as you go. You can then use the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create Cisco Unity subscriber accounts.

Note If mailboxes for Cisco Unity subscribers will be homed in Exchange 2007, you cannot use Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create new Active Directory accounts at the same time that you create subscriber accounts. You must create Active Directory accounts and Exchange mailboxes before you create Cisco Unity subscriber accounts.

- Use the Cisco Unity Administrator to add subscribers one at a time. Use a different template for each subscriber that you create, specifying a unique and secure Active Directory password in each template. Alternatively, you can use one template for all subscribers, but specify a unique and secure password before each subscriber account that you add. If you use the same template for all subscribers, you will need to record the passwords that you assign to each subscriber in a secure place so that you can distribute them later. (Cisco Unity stores only the last value saved.)

Before you specify a template password, review the password policy for the Active Directory domain to make sure that the minimum length and complexity requirements do not conflict with the password that you specify in the template. Cisco Unity will not add a subscriber account when the length of the password on the subscriber template is less than the minimum length for passwords in the Active Directory domain.

Assigning Unique and Secure Active Directory Passwords After Subscriber Accounts Have Been Created

After you have created subscriber accounts, use one of the following methods to assign each account a unique and secure Active Directory password:

- Use Active Directory Users and Computers to change the existing password for each user.
- Ask subscribers to change their own passwords. Subscribers can change their Cisco PCA passwords in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is on a different domain than the one that subscribers typically access, subscribers will also need to specify the domain name for the Cisco Unity server.)

  Note that subscribers may assume that their phone and Cisco PCA passwords are the same. As a result, they may think that they are changing both passwords when Cisco Unity prompts them to change their phone password during first-time enrollment. For this reason, you may find that many subscribers do not change their Cisco PCA passwords in Windows, even though you request that they do so.

Where Cisco Unity Data Is Stored

Cisco Unity stores information about subscriber accounts in a SQL Server database on the Cisco Unity server. In addition, a small subset of subscriber account information is also stored in Active Directory. During installation, the Active Directory schema is extended to store subscriber account information.

For additional information on how data is stored in Cisco Unity, see the *White Paper: Cisco Unity Data and the Directory (All Versions with Microsoft Exchange)*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_white_paper09186a00800875c5.shtml.

Importing User Data from Other Routing Groups

Although you can use the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator to import user data from other Exchange routing groups, you should do so only if there is a high-bandwidth connector between the groups that can support message streaming.

Setting Up Regular Cisco Unity Subscribers to Use Bridge Networking

If your installation includes the Bridge Networking option, in order for Cisco Unity subscribers to be able to send messages to and receive messages from subscribers on the Octel servers with which Cisco Unity communicates, each Cisco Unity subscriber account must be configured with an Octel serial number and a remote mailbox number. This allows the remaining Octel subscribers to address messages by using the same number that they used before the subscriber migrated to Cisco Unity.

The combination of serial number and mailbox number uniquely identifies a subscriber within an Octel analog network. For each serial number, the legacy mailbox number must be unique within the global directory. If you are creating Cisco Unity subscriber accounts for users who previously existed on an Octel system, use the serial number of the Octel server that the subscriber migrated from and the mailbox

number that the subscriber had on the Octel system. If you are creating Cisco Unity subscriber accounts for new users who were never subscribers on an Octel system, choose a serial number and a mailbox number that is not already in use.

You can add the serial number and mailbox number as you create subscriber accounts by using either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator. You can also use these same tools to add the serial and mailbox numbers to existing subscriber accounts.

For directory data about newly-created subscribers to be automatically sent to the Bridge, you first create the subscribers in Cisco Unity, and then create corresponding Unity Node(s) on the Bridge. If you do the reverse and create a Unity Node on the Bridge before creating any subscribers with the same serial number, you will have to force a synchronization by going to the Network > Bridge Options > Synchronization Options page to send directory data to the Bridge, or delete and then add back in the Unity Node on the Bridge. Subsequently, if you add more subscribers with the same serial number, Cisco Unity automatically sends the directory information to the Bridge.

Adding the serial and mailbox numbers to Cisco Unity subscriber accounts is just one of the steps required to properly configure Bridge Networking. For more information, see the applicable *Networking Guide for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts

The Cisco Unity Bulk Import wizard allows you to create multiple subscriber accounts at once either by importing user data directly from Active Directory or by importing user data contained in a comma-separated value (CSV) file.

Importing User Data Directly from a Message Store Directory

When you use the Cisco Unity Bulk Import wizard to import user data directly from the message store directory, Cisco Unity uses the mailbox data and Active Directory account information to create the Cisco Unity subscriber account.

However, Cisco Unity does not enable Active Directory accounts if they are disabled at the time that you import mailbox data from Exchange.

This is important because Active Directory credentials are required to access the Cisco Personal Communications Assistant (PCA), the Cisco Unity Administrator, and to use the phone as a recording and playback device for the Media Master. To allow subscribers to access these applications, enable Active Directory accounts before you use the Cisco Unity Bulk Import wizard to import data from the message store directory.

Finally, the Cisco Unity Bulk Import wizard requires each regular subscriber to have a DTMF_ACCESS_ID that callers can use to reach the subscriber. Typically, the DTMF_ACCESS_ID is the same as the subscriber extension. Before running the Cisco Unity Bulk Import wizard, print out a list of the user names that you plan to import, and specify a DTMF_ACCESS_ID for each user. The ID must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one. Save this list to use when you enter any missing DTMF_ACCESS_IDs during the import process.

If your installation includes the Bridge Networking option, in order for Cisco Unity subscribers to be able to send messages to and receive messages from subscribers on the Octel servers with which Cisco Unity communicates, each Cisco Unity subscriber account must be configured with an Octel serial

number and a remote mailbox number. Before running the Cisco Unity Bulk Import wizard, gather the serial and mailbox numbers for the subscriber accounts that you will be creating. During the import process, you enter the numbers in the REMOTE_NODE_ID and LEGACY_MAILBOX columns in the displayed grid on the Select Data to Import dialog box. Note that the Cisco Unity numbering plan is independent of the numbering plan on the Octel system; therefore, the numbers that you enter for LEGACY_MAILBOX and DTMF_ACCESS_ID for each subscriber may or may not be the same. For more information about REMOTE_NODE_ID and LEGACY_MAILBOX, see the Cisco Unity Bulk Import wizard Help.

When you are ready to create subscribers by importing user data directly from the message store directory, see the "Running the Cisco Unity Bulk Import Wizard" section on page 21-23.

Importing User Data From a CSV File

CSV is a common text file format for moving data from one data store to another. In particular, importing from a CSV file is helpful when you want to create subscriber accounts based on user data from voice messaging systems that run on different operating systems, or that have different database structures than Cisco Unity. As long as the user data contained in the CSV file is formatted as indicated in this section, you can use it with the Cisco Unity Bulk Import wizard to create subscriber accounts with or without existing Exchange mailboxes and Active Directory accounts.

Using the Create New Mailboxes and Windows Accounts Option

If the users in your CSV file do not already have Exchange mailboxes and Active Directory accounts, you can create them at the same time that you create Cisco Unity subscriber accounts. (If mailboxes for Cisco Unity subscribers will be homed in Exchange 2007, you do not have this option. You must create Active Directory accounts and Exchange mailboxes before you create Cisco Unity subscriber accounts.) The Cisco Unity Bulk Import wizard creates the mailbox in the message store and on the server that you specify on the pages of the wizard. The Active Directory account is created in the domain and organizational unit (OU) that you specify.

Note In some cases, you may want the Active Directory accounts that Cisco Unity creates to be disabled. For more information, see the "How Cisco Unity Handles Active Directory Accounts for the Subscriber Accounts That You Create" section on page 21-5.

Note that if a user already exists with the same alias as the subscriber that you want to create, the Cisco Unity Bulk Import wizard notifies you that it cannot create the subscriber or the Exchange mailbox. This may happen if your CSV file contains a user that already has an Exchange mailbox. To create the subscriber account in such cases, use the Use Existing Mailboxes and Windows Accounts option to import the mailbox data for the user instead.

Note If you have not done so already, consider password security if you plan to create new Active Directory accounts at the same time that you create subscribers. See the "Ensuring That Subscribers Are Assigned Unique and Secure Active Directory Passwords" section on page 21-7 for details.

Using the Existing Mailboxes and Active Directory Accounts Option

When you create subscriber accounts for users with existing Exchange mailboxes, Cisco Unity uses the mailbox data and Active Directory account information to create the Cisco Unity subscriber account. However, Cisco Unity does not enable Active Directory accounts if they are disabled at the time that you import mailbox data from Exchange.

This is important because subscribers whose Active Directory account is disabled cannot access the Cisco Personal Communications Assistant (PCA) or the Cisco Unity Administrator, or use the phone as a recording and playback device for the Media Master. To avoid this problem, enable Active Directory accounts before you use the Cisco Unity Bulk Import wizard to import data from your CSV file.

The first row in your CSV file must contain column headers that identify the type of data in each column; information in the subsequent rows must contain the data that you want to import. Column headers must be in uppercase, separated by commas, and spelled as shown in the tables in the following sections:

- Required Column Headers, page 21-11
- Optional Column Headers, page 21-13

In addition, make sure that commas separate the data in each row in your CSV file, including the column headers in the first row. Do not use a tab, spaces, or a semicolon to separate values in the file. Finally, if any data includes a space, quotes, or commas, contain it within quotes.

Required Column Headers

The required column headers for regular subscribers are shown in Table 21-1. Note that the column headers are shown in the order in which they should appear in your CSV file.

Note When you select the Use Existing Mailboxes and Windows Accounts option, the only required column headers for a CSV file are ALIAS and DTMF_ACCESS_ID. If left unspecified in the CSV file, the subscriber first names, last names, and display names are imported from directory. Otherwise, the Cisco Unity Bulk Import wizard overwrites the directory with the first names, last names, and/or display names when they are specified in the CSV file.

Table 21-1 Required CSV Headers for Regular Subscribers

Column Header	Description
LAST_NAME	Subscriber last name. Enter any combination of letters, digits, spaces, apostrophes, and dashes, up to a maximum of 32 characters.
FIRST_NAME	Subscriber first name. Enter any combination of letters, digits, spaces, apostrophes, and dashes, up to a maximum of 32 characters.
DTMF_ACCESS_ID *(when you select the Use Existing Mailbox and Windows Account option, only this column header and ALIAS are required)*	The number that callers dial to reach a subscriber. This value corresponds to the Extension field on the Subscribers > Subscribers > Profile Page page in the Cisco Unity Administrator. Enter any combination of digits from 0 to 9, up to a maximum of 40 digits. Do not include any spaces. Note that the value must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.

Table 21-1 Required CSV Headers for Regular Subscribers (continued)

Column Header	Description
ALIAS *(when you select the Use Existing Mailbox and Windows Account option, only this column header and DTMF_ID are required)*	The Cisco Unity Bulk Import wizard searches for the Exchange mailbox that matches the alias entered here. The matching Exchange mailbox will be associated with the subscriber account. If you do not specify an alias here, the Exchange alias for the created account will be derived from a rule specified in the subscriber template, by using a combination of first and last name. Typically, you enter an alias here in order to override the alias generation rule (for example, when there are users who need to have aliases that do not follow the convention, such as when there is a naming conflict). Enter any combination of letters, digits, periods, underscores, or dashes, up to a maximum of 64 characters. The first 20 characters of the alias must be unique (they must not exactly match the first 20 characters of any other new or existing alias in the directory).
LEGACY_MAILBOX *(required only when using the Bridge Networking option for messaging with Octel subscribers)*	The number used to identify a Cisco Unity subscriber on a node in an Octel analog network. This number is required for all Cisco Unity subscribers who will be messaging with subscribers on an Octel system via the Cisco Unity Bridge. Without a LEGACY_MAILBOX number, a Cisco Unity subscriber cannot send messages to or receive messages from Octel subscribers. When you create Cisco Unity subscriber accounts for users who are migrating from Octel, enter the mailbox number that the subscriber had on the Octel system. This allows the remaining Octel subscribers to address messages by using the same number that they used before the subscriber was migrated. For existing Cisco Unity subscribers (including subscribers who have already migrated from Octel in a previous version of Cisco Unity and the Bridge), you can run the Cisco Unity Bulk Import wizard to add the LEGACY_MAILBOX number to each subscriber account. Enter the number that Octel subscribers dial to address messages to the Cisco Unity subscriber (excluding the location Dial ID or prefix). Enter any combination of digits from 0 to 9. Do not include any spaces. Typical mailbox numbers contain 3 to 10 digits (although the Cisco Unity Bulk Import wizard accepts a maximum of 64 digits). Note that the LEGACY_MAILBOX and the DTMF_ACCESS_ID do not have to be the same number. When using this column, you must also include the REMOTE_NODE_ID column. The combination of the REMOTE_NODE_ID and LEGACY_MAILBOX uniquely identifies a subscriber within an Octel analog network. If a record contains data in one column but not the other, the Cisco Unity Bulk Import wizard logs an error, and the subscriber account is not created. For each REMOTE_NODE_ID, the LEGACY_MAILBOX value must be unique within the global directory. If the Cisco Unity Bulk Import wizard detects a duplicate REMOTE_NODE_ID and LEGACY_MAILBOX pair in the CSV file, or if an existing Cisco Unity subscriber has a matching REMOTE_NODE_ID and LEGACY_MAILBOX, the Cisco Unity Bulk Import wizard logs an error, and the subscriber account is not created.

Table 21-1 Required CSV Headers for Regular Subscribers (continued)

Column Header	Description
REMOTE_NODE_ID *(required only when using the Bridge Networking option for messaging with Octel subscribers)*	In an Octel analog network, the serial number of the node with which the Cisco Unity subscriber is associated. This number is required for all Cisco Unity subscribers who will be messaging with subscribers on an Octel system via the Cisco Unity Bridge. Without a REMOTE_NODE_ID number, a Cisco Unity subscriber cannot send messages to or receive messages from Octel subscribers. When you create Cisco Unity subscriber accounts for users who are migrating from Octel, enter the serial number of the Octel node that the subscriber is migrating from. For existing Cisco Unity subscribers (including subscribers who have already migrated from Octel in a previous version of Cisco Unity and the Bridge), you can run the Cisco Unity Bulk Import wizard to add the REMOTE_NODE_ID to each subscriber account. Enter the serial number of a Unity Node that has been configured in the Bridge Administrator. Enter any combination of digits from 0 to 9. Do not include any spaces. Typical serial numbers contain 4 or 5 digits (although the Cisco Unity Bulk Import wizard accepts a maximum of 64 digits). When using this column, you must also include the LEGACY_MAILBOX column. The combination of the REMOTE_NODE_ID and LEGACY_MAILBOX uniquely identifies a subscriber within an Octel analog network. If a record contains data in one column but not the other, the Cisco Unity Bulk Import wizard logs an error, and the subscriber account is not created. For each REMOTE_NODE_ID, the LEGACY_MAILBOX value must be unique within the global directory. If the Cisco Unity Bulk Import wizard detects duplicate REMOTE_NODE_ID and LEGACY_MAILBOX values in the CSV file, or if an existing Cisco Unity subscriber has a matching REMOTE_NODE_ID and LEGACY_MAILBOX, the Cisco Unity Bulk Import wizard logs an error, and the subscriber account is not created.

Optional Column Headers

There are a number of optional column headers that you can include in your CSV file, as shown in Table 21-2. Most optional column headers correspond to subscriber settings defined in the subscriber template, including class of service (COS), call transfer, and message notification settings. When data for a particular subscriber setting is not included in the CSV file, the Cisco Unity Bulk Import wizard uses settings in the subscriber template that you choose when you run the Cisco Unity Bulk Import wizard. For this reason, you should review the settings in the subscriber template that you will use to create the accounts before adding any of the optional column headers to your CSV file.

Use Table 21-2 to learn more about the optional column headers that you can include in the CSV file. Unless otherwise indicated, all optional column headers can be used to define any type of subscriber account.

Table 21-2 Optional CSV File Column Headers

Optional Column Header	Description
ALIAS **Note** This column header is optional only if you choose to create new directory objects at the same time that you create subscriber accounts. The column header is required when you create subscriber accounts with existing directory objects.	The Cisco Unity Bulk Import wizard searches for the directory objects (Exchange mailbox and Active Directory account for regular subscribers, contact or custom recipient for AMIS, Bridge, Internet, and VPIM subscribers) that match the alias entered here. The matching directory objects will be associated with the subscriber account. If you do not specify an alias here, the alias for the created account will be derived from a rule specified in the subscriber template, using a combination of first and last name. Typically, you enter an alias here in order to override the alias generation rule (for example, when there are users who need to have aliases that do not follow the convention, such as when there is a naming conflict). Enter any combination of letters, digits, periods, underscores, or dashes, up to a maximum of 64 characters. The first 20 characters of the alias must be unique (they must not exactly match the first 20 characters of any other new or existing alias in the directory).
ALTERNATE_EXTENSION_1	In addition to the "primary" extension that you assign subscribers, you can also assign alternate extensions. The extensions that you add are appended to the Administrator-Defined Alternate Extensions table on the Subscribers > Alternate Extension page in the Cisco Unity Administrator. Consider the following when you enter alternate extensions: • You can enter an extension up to 40 characters in length. (SIP integrations can use up to 40 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.
AUDIO_SPEED	Defines the speed of message playback. • 0—Low speed. • 100—Medium speed (default value). • 200—Fast speed.
AUDIO_VOLUME	Indicates the volume for message playback. • 0—Low volume. • 50—Medium volume (default value). • 100—High volume.
CALLERS_LANGUAGE	The language of the Cisco Unity conversation that callers hear when they call a subscriber. Enter any combination of letters and digits, up to a maximum of four characters.
CONVERSATION_NAME	The Cisco Unity conversation that the subscriber hears when retrieving messages. Enter any combination of letters and digits, up to a maximum of 64 characters.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
COS_OBJECT_NAME	The name of the subscriber class of service (COS) of which the subscriber will be a member. The COS must already exist in the Cisco Unity Administrator. Enter any combination of letters, digits, and braces, up to a maximum of 128 characters. Enter the name of the COS as it appears in the Cisco Unity Administrator.
DELIVERY_LOCATION_ID *(AMIS, Bridge, and VPIM subscribers only)*	The dial ID of a delivery location that the external subscriber will be associated with. This value corresponds to the Dial ID field on the Network > Delivery Locations > Profile page in the Cisco Unity Administrator. If this column header is omitted, or if a row does not contain a value, the delivery location that the Cisco Unity Bulk Import wizard prompts for is used as a default. You can import external subscribers for multiple delivery locations by using one CSV file. Enter any combination of digits from 0 through 9, up to a maximum of 64 digits.
HIDE_IN_ADDRESS_BOOK	Specify whether you want to prevent subscribers from appearing in the Outlook address book. When you prevent subscribers from appearing in Outlook address books, Exchange will still deliver e-mail messages addressed to them, but the number of messages may be reduced because other subscribers cannot use the Outlook address book to address messages to them. When a value is entered in this column, the Cisco Unity Bulk Import wizard overwrites the values in the following fields: • The Show Subscriber in E-Mail Server Address Book field on the Subscribers > Subscriber > Profile page in the Cisco Unity Administrator. • The Hide From Exchange Address Lists field on the Exchange Advanced tab for each user in Active Directory Users and Computers. Enter 0 or 1: • 0—Display subscriber in the Outlook address book. • 1—Hide subscriber from the Outlook address book.
DISPLAY_NAME	Specifies the display name for the subscriber. The format selected here should be consistent with the Exchange name generation rule for existing Exchange mailboxes. When no display name is specified, it is constructed in one of the following ways, as applicable: • The first and last names as specified in the message store. • The first and last names as specified in the rule in the subscriber template that is selected during the import. Enter any combination of letters, digits, spaces, periods, commas, apostrophes, or other characters—including dashes, up to a maximum of 64 characters.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
DOMAIN_LOCATION *(regular subscribers only)*	Specifies the Windows NT 4.0 domain name in which the alias in the NT40_ALIAS column can be found. Use this column if you are creating subscriber accounts for users who have both a Windows NT 4.0 account and an Active Directory account, or if your organization is in the process of moving users from Windows NT 4.0 to Active Directory, or from one Active Directory domain to a new domain. In addition, you need to specify the alias in the column NT40_ALIAS so that the Cisco Unity Bulk Import wizard can find the Windows NT 4.0 account information to associate with the subscriber. Without associated Windows domain accounts, the subscriber accounts that you create will not have access to the Cisco Unity Administrator or the Cisco Personal Communications Assistant (PCA), and cannot use the phone as the recording and playback device for the Media Master. Enter any combination of letters, up to a maximum of 15 letters.
DTMF_ACCESS_ID *(optional for Internet subscribers only; required for regular, AMIS, Bridge, and VPIM subscribers)*	The number that callers dial to reach a subscriber. This is also the extension that subscribers on the local Cisco Unity server use to address messages to AMIS, Bridge, Internet, or VPIM subscribers. This value corresponds to the Extension field on the Subscribers > Subscribers > Profile page in the Cisco Unity Administrator. Enter any combination of digits from 0 through 9, up to a maximum of 40 digits. Do not include any spaces. Note that the value must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.
DTMF_PASSWORD	The password that governs how subscribers initially log on to Cisco Unity by phone. This value corresponds to the Password field on the Subscribers > Subscriber > Passwords page in the Cisco Unity Administrator. By default, subscriber templates use 12345 as the default phone password for all subscribers unless you change it in the template or change it here. To help protect Cisco Unity from unauthorized access and toll fraud, the password should be changed. (Note that if your system is a new installation, this task may have already been done, because the installer is prompted to change the default phone password for the {Default Subscriber} template during installation. However, if your system was upgraded from a Cisco Unity version prior to 4.0(4), the installer was not prompted to change the password during installation.) Enter any combination of digits from 0 through 9, up to a maximum of 20 digits. As a best practice, specify a long—eight or more digits—and non-trivial password. (Requirements for password complexity are set on the Subscribers > Account Policy > Phone Password Restrictions page in the Cisco Unity Administrator.)
LIST_IN_DIRECTORY	Determines whether the subscriber is listed in the phone directory. • 0—Turns directory listing off. • 1—Turns directory listing on.
MAX_MSG_LENGTH	Indicates the maximum length of voice mail messages (in seconds) that unidentified callers can leave. Enter any value from 0 to 999 seconds.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
MWI_EXTENSION_1	The message waiting indicator (MWI) extension, if different from phone extension for the subscriber. Enter any combination of digits from 0 through 9 for the extension , and "," (comma) or ";" (semi-colon) for pause, for a maximum of 40 characters.
NOTES	The Cisco Unity Bulk Import wizard ignores a column with this header. The Cisco Unity Bulk Import wizard does not support more than one NOTES column in a CSV file. Enter any comments that you may have for this record. Enter any combination of letters, characters, and digits, for a maximum of 255 characters.
NT40_ALIAS	Specifies the Windows NT 4.0 alias. Use this column if you are creating subscriber accounts for users who have both a Windows NT 4.0 account and Windows 2000 account, or if your organization is in the process of moving users from Windows NT 4.0 to Windows 2000, or from one Active Directory domain to a new domain. In addition, you need to specify the domain name in the column DOMAIN_LOCATION so that the Cisco Unity Bulk Import wizard can find the Windows NT 4.0 account information to associate with the subscriber. Without associated Windows domain accounts, the subscriber accounts that you create will not have access to the Cisco Unity Administrator or to the Cisco Personal Communications Assistant (PCA), and cannot use the phone as the recording and playback device for the Media Master. Enter any combination of letters and digits, up to a maximum of 40 characters.
PAGER1_NUMERIC_AFTER_DIAL_DIGITS *(regular subscribers only)*	The extra digits that Cisco Unity dials after the phone number for a message notification. The extra digits are shown on the pager display. This column corresponds to the Extra Digits field for the Pager device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Enter any combination of digits from 0 through 9, up to a maximum of 32 digits.
PAGER1_NUMERIC_DIAL_DELAY *(regular subscribers only)*	Specifies the number of seconds to wait before dialing the extra digits specified in the PAGER1_NUMERIC_AFTER_DIAL_DIGITS column. Use this option if the automatic call progress detection of your phone system is not reliable (for example, if you experience noisy phone lines and unusual ringing patterns). This column corresponds to the Seconds to Wait Before Dialing Extra Digits field for the Pager device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Enter any value from 0 to 100 seconds.
PAGER1_NUMERIC_DISABLE	Disables the numeric pager device. This column corresponds to the Status field for the Pager device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Enter 1. After you create the subscriber accounts, you can enable the pager in the Cisco Unity Administrator, or you can tell subscribers to do so in the Cisco Unity Assistant.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
PAGER1_NUMERIC_PHONE_NO *(regular subscribers only)*	The phone number, including trunk access code, of the numeric pager to be used for message notifications. This column corresponds to the Phone Number field for the Pager device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled during import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant. Enter any combination of digits from 0 through 9, and the following dialing characters, up to a maximum of 40 characters: • , (comma) to insert a one-second pause. • # and * to correspond to the # and * keys on the phone.
PAGER1_TEXT_AFTER_DIAL_DIGITS *(regular subscribers only)*	Specifies a phone number if the subscriber has a text-compatible cell phone and wants text pager notifications to include a “From” or “Return Call” phone number. Typically, this field contains the number of the Cisco Unity server that the subscriber calls to check messages. The From phone number appears in the last line of any text pager notification. A subscriber can press the Return Call button on many text-compatible cell phones to dial the phone number. The cell phone must support automatic callback in order to use this feature. This column corresponds to the From: (Phone Number) field for the Text Pager 1 device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Enter any combination of digits, up to a maximum of 32 digits.
PAGER1_TEXT_DISABLE	Disables the text pager device. This column corresponds to the Status field for the Text Pager 1 device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Enter 1. After you create the subscriber accounts, you can enable the pager in the Cisco Unity Administrator, or you can tell subscribers to do so in the Cisco Unity Assistant.
PAGER1_TEXT_SMTP_ADDRESS *(regular subscribers only)*	Specifies the e-mail address of the text pager, text-compatible cell phone, or another e-mail account (such as a home e-mail address) to which message notifications will be sent. This column corresponds to the To: (E-Mail Address) field for the Text Pager 1 device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled during import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant. Enter any combination of letters, digits, colons, ampersands, dashes, periods, and underscores, up to a maximum of 128 characters.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
PUBLIC_DL	Specifies the public distribution lists to which new subscribers are added. This column corresponds to the Subscribers > Subscriber > Distribution Lists page in the Cisco Unity Administrator. By default, subscriber templates assign new subscribers to the All Subscribers list. Use this column to add subscribers to distribution lists that are not already specified in the template; lists that you enter in this column do not overwrite any lists specified in the template. Enter any combination of letters, digits, spaces, periods, semicolons, commas, or most other characters—including apostrophes and underscores—up to 255 characters. Separate each public distribution list name with a semicolon. For example, you can enter "All Subscribers; Accounting Department."
SUBSCRIBER_TEMPLATE	The subscriber template that you want to associate the subscribers with when they are created. Enter any combination of letters and digits, up to a maximum of 128 characters.
SUBSCRIBERS_LANGUAGE	The language that the subscriber hears when logging on to Cisco Unity by phone. Enter any combination of letters and digits, up to a maximum of four characters.
TIME_EXPIRES	Specifies the date that call transfer is turned off for the subscriber extension. If the value is 0 (zero), call transfer is turned on, and because there is no expiration date, it never turns off. If the value is a date in the past (for example, 01/01/80), call transfer is turned off. Enter a valid date in the format of mm/dd/yy, yy/mm/dd, or enter 0 (zero).
TRANSFER_STRING	Specifies the call transfer number for the subscriber. The value is usually the same as the DTMF_ACCESS_ID (so that Cisco Unity sends calls to the subscriber extension), though the value for the dialing transfer string can be left blank. This corresponds to the Transfer Incoming Calls to Subscriber's Phone field on the Subscribers > Subscribers > Call Transfer page in the Cisco Unity Administrator. Enter any combination of digits from 0 through 9, up to a maximum of 40 digits, and the following dialing characters: • , (comma) to insert a one-second pause. • ; (semi-colon) to insert a pause. Transfer options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.
USE_BRIEF_PROMPTS	Indicates whether the subscriber hears brief or full phone menus when accessing Cisco Unity over the phone. • 0—Turns brief menus on. • 1—Turns full menus on.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
VMI_TEXT_SMTP_ADDRESS *(regular subscribers only)*	Use to set up a text message notification so that Cisco Unity Inbox subscribers who do not use ViewMail for Outlook will receive an e-mail when a new voice message arrives. Enter the e-mail address of the subscriber text pager, text-compatible cell phone, or another e-mail account (such as a home e-mail address). This column corresponds to the To: (E-Mail Address) field for the Text for Cisco Unity Inbox device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled during import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant. Note that you can enter the URL for the Cisco Personal Communications Assistant (PCA) on the System > Configuration page in the Cisco Unity Administrator, so that it is automatically included as a link in the body of the e-mail message that is sent to the subscriber. (Subscribers use the Cisco PCA to access their Cisco Unity Inboxes.) Enter any combination of letters, digits, colons, ampersands, dashes, periods, and underscores, up to a maximum of 128 characters.
VMI_TEXT_AFTER_DIAL_ DIGITS *(regular subscribers only)*	Use to set up a text message notification so that Cisco Unity Inbox subscribers who do not use ViewMail for Outlook receive an e-mail when a new voice message arrives. Enter a phone number if the subscriber has a text-compatible cell phone and wants message notifications to include a return phone number. Typically, this field contains the number that the subscriber calls to check messages. This column corresponds to the To: (E-Mail Address) field for the Text for Cisco Unity Inbox device on the Subscribers > Subscribers > Message Notification page in the Cisco Unity Administrator. Message notifications to this device are disabled during import and must be enabled in the Cisco Unity Administrator or by the subscriber in the Cisco Unity Assistant. Note that you can enter the URL for the Cisco Personal Communications Assistant (PCA) on the System > Configuration page in the Cisco Unity Administrator, so that it is automatically included as a link in the body of the e-mail message that is sent to the subscriber. (Subscribers use the Cisco PCA to access their Cisco Unity Inboxes.) Enter any combination of digits, up to a maximum of 32 characters.
VOICE_NAME	Specifies the full path to a WAV audio file containing the recorded voice name of the subscriber. The audio file should have been recorded in a codec playable on all Cisco Unity servers in the network; no codec checking or conversion is done during the import. Enclose the path in quotes if it contains any space characters.
XFER_ANNOUNCE	Defines whether Cisco Unity says “transferring call” when subscribers answer calls that were transferred from the automated attendant or a directory handler. For this to work, XFER_TYPE must be set to “supervised.” • 0—Turns announce off. • 1—Turns announce on. Screening options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
XFER_CONFIRM	Defines whether Cisco Unity asks subscribers if they would like to take calls transferred from the automated attendant or a directory handler. For this to work, XFER_TYPE must be set to "supervised." • 0—Turns confirm off. • 1—Turns confirm on. Screening options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.
XFER_HOLDING_MODE	Determines whether the caller can be put on hold when an extension is busy. For this to work, XFER_TYPE must be set to "supervised." • 0—Turns call holding off. • 1—Turns call holding on. Holding options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.
XFER_INTRODUCE	Defines whether subscribers hear "call for <the recorded voice name of the subscriber>," or "call for <extension number>," when they answer calls transferred from the automated attendant or a directory handler. Used when two or more subscribers share a phone. For this to work, XFER_TYPE must be set to "supervised." • 0—Turns introduce off. • 1—Turns introduce on. Screening options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.
XFER_RINGS	When doing a supervised transfer, the number of rings to wait before activating the applicable call handler. Enter any digit from 1 to 9.
XFER_SCREENING	Sets call screening to off, on, or on with "memory" (the recorded name of the caller is added to the message). For this to work, XFER_TYPE must be set to "supervised." • 0—Turns call screening off. • 1—Turns call screening on. • 2—Turns call screening on with memory. Screening options apply to calls transferred from the automated attendant or a directory handler; they do not apply when an outside caller or another subscriber dials a subscriber extension directly.
XFER_TYPE	Used in conjunction with RNA_ACTION to determine whether Cisco Unity monitors the progress of a call until the subscriber answers the phone. • 0—Unsupervised transfer; Cisco Unity does not monitor call progress. • 1—Supervised transfer; Cisco Unity monitors call progress.

Table 21-2 Optional CSV File Column Headers (continued)

Optional Column Header	Description
ZERO_KEY_RULE *(regular subscribers only)*	Specifies the display name for the call handler to which calls to this subscriber are transferred when unidentified callers press "0" during the subscriber greeting. This allows calls to different groups of subscribers to be handled by different operators. Note that the Cisco Unity Bulk Import wizard checks to see whether the name is a valid call handler. Therefore, the call handler must have been created in the Cisco Unity Administrator before doing the import. Enter any combination of letters, digits, periods, spaces, dashes, or other characters—including underscores—up to a maximum of 128 characters.

After reviewing Table 21-1 and Table 21-2, use the following procedure to prepare your CSV file.

To Prepare a CSV File for Creating Regular Subscriber Accounts

Step 1 Save the data that you will use to create Cisco Unity accounts as a CSV file.

As a best practice, do not include more than 7,500 records in a single CSV file, as you may encounter unexpected results when the Cisco Unity Bulk Import wizard imports the data.

Step 2 Copy the CSV file to the Cisco Unity server or to a folder that you can browse to from the server.

Step 3 Open the CSV file in a spreadsheet application or another application with which you can edit and reorganize the data. Do the following:

- Confirm that the data is separated by commas, and that no tabs, spaces, or semicolons separate the data in the file.
- If any data includes a space, quotes, or commas, contain it within quotes.

Step 4 Rearrange the data, so that the columns are in the same order as the column headers that you will add in Step 5. The order of the column headers does not matter, though it is good practice to set up your CSV file as indicated here. For example, the columns of data in this sample are sorted so that the last name of the user is followed by the first name and then by the DTMF_ACCESS_ID:

Abade,Alex,2001
Bader,Kelly,2002

Step 5 Enter the required column headers above the first row of data. Column headers must be uppercase, separated by commas, and spelled as indicated in Table 21-1.

For example, the column headers for the sample data from Step 4 would look like this:

LAST_NAME,FIRST_NAME,DTMF_ACCESS_ID

Step 6 If applicable, add any of the optional column headers listed in Table 21-2 to the first row, and the corresponding data that you want to import in the subsequent rows below. As you do so, confirm that:

- Column headers and data are separated by commas. Note that each row does not have to contain data for each optional column header.
- Any data that includes a space, quotes, or commas is contained within quotes.

Step 7 If your CSV file contains columns of data that you do not want to import, delete the columns. Alternatively, you can title one column NOTES. The Cisco Unity Bulk Import wizard ignores data beneath a NOTES column header, but the wizard does not support more than one NOTES column in a CSV file.

Step 8 Confirm that each row contains the applicable data corresponding to each column header.

Step 9 Save the file as a CSV file.

Step 10 Continue with the procedure in the "Running the Cisco Unity Bulk Import Wizard" section on page 21-23.

Running the Cisco Unity Bulk Import Wizard

Do the procedure in this section to use the Cisco Unity Bulk Import wizard to create multiple subscriber accounts. Do so only after you have reviewed the following sections:

- Issues to Consider Before Creating Regular Subscriber Accounts, page 21-2
- Importing User Data Directly from a Message Store Directory, page 21-9 (as applicable)
- Importing User Data From a CSV File, page 21-10 (as applicable)

For best results, note the following:

- Do not attempt to create more than 7,500 new subscriber accounts at once. If you have more than 7,500 users for whom you want to create Cisco Unity subscriber accounts, run the Cisco Unity Bulk Import wizard multiple times.
- After the wizard has created a subscriber account for a particular user, it will not process the data for that user when it is run again.
- You can create only one type of subscriber account each time that you run the Cisco Unity Bulk Import wizard.
- The Cisco Unity Bulk Import wizard can import user data from only one message store directory at a time.

When the Cisco Unity Bulk Import wizard initially loads the Exchange user data or the records in your CSV file, it examines the data for errors. If an error is found, the wizard notifies you and logs the error in the error.log file. You can choose either to ignore the error and correct it later, or you can correct the error, and start the wizard again. After it creates subscriber accounts, the wizard displays a dialog box that reports the results of loading the data, including the number of records found, the number of records successfully loaded, and the number of records that still have errors.

Use the following procedure to use the Cisco Unity Bulk Import wizard to create regular subscriber accounts, and to manage any errors that the wizard discovers in the process.

Note Before you run the Cisco Unity Bulk Import wizard, disable virus-scanning services and intrusion-detection software on the Cisco Unity server, if applicable. Otherwise, the Cisco Unity Bulk Import wizard may run slowly. See Cisco Unity Bulk Import wizard Help for procedures.

To Create Regular Subscribers by Using the Cisco Unity Bulk Import Wizard

Step 1 On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.

Step 2 Follow the on-screen instructions presented on each page of the wizard.

To learn more about the options presented in the dialog boxes that appear as the wizard proceeds, click **Help**.

Step 3 When prompted to choose the type of subscriber that you want to create, click **Unified Messaging** or **Voice-Mail Only**.

Step 4 Click **Next**, and proceed through the wizard. If the wizard reports any errors, you can:

- Click **OK** to continue with the import, and fix the errors later.
- Fix the errors. See the "Correcting Import Errors" section on page 21-24 for details.

Step 5 If you are importing user data directly from the message store directory, confirm that there is a DTMF_ACCESS_ID specified for each user on the Select Data to Import page.

Enter the applicable data in the grid if a DTMF_ACCESS_ID is not specified for a user:

- Enter digits only.
- Typically, the DTMF_ACCESS_ID is the same as the subscriber extension. Therefore, the data you enter should be consistent with the extension numbering plan used in your organization.
- The ID must be unique among all extensions on the local Cisco Unity server and within the dialing domain, if there is one.

Step 6 When the subscriber accounts are created, click **Finish**.

Step 7 If you had import errors, but in Step 4 you chose to correct them later, see the "Correcting Import Errors" section on page 21-24.

If you had no import errors, or if all errors have now been corrected, see the "Issues to Consider After Creating Subscriber Accounts" section on page 21-28.

Correcting Import Errors

The error log file contains data that the Cisco Unity Bulk Import wizard could not import. The Cisco Unity Bulk Import wizard reports the first error it detects in any user mailbox or row in a CSV file. After you correct that error, the Cisco Unity Bulk Import wizard may detect additional errors in the same mailbox or row when the data is imported again. Thus, you may need to repeat the correction process—running the Cisco Unity Bulk Import wizard and correcting an error—several times to find and correct all errors.

The output log file contains all of the records that were not imported. You can save it as a CSV file, and use it when you run the Cisco Unity Bulk Import wizard again. Note that each time that you run the Cisco Unity Bulk Import wizard, the error and output log files are overwritten (unless you specify a new name for the files each time you run it).

To correct import errors, use one of the two procedures below.

To Correct Errors That Occurred When Importing Data from the Message Store

Step 1 Go to the directory location of the error log file you specified during the import. (The default location and file name is **C:\Error.log**.)

Step 2 Use a text editor to open the error log file. You will use the error codes in the file to make corrections.

Step 3 When importing data from Exchange, open **Active Directory Users and Computers**.

Step 4 Double-click a mailbox that contains an error to see the properties.

Step 5 Enter corrections in the applicable boxes in the mailbox.

Step 6 Click **OK**.

Step 7 Repeat Step 4 through Step 6 for each mailbox listed in the error log file.

Step 8 Run the Cisco Unity Bulk Import wizard again.

Step 9 Repeat this procedure until all subscriber accounts are created without error, and then proceed to the "Issues to Consider After Creating Subscriber Accounts" section on page 21-28.

To Correct Errors That Occurred When Importing Data from a CSV File

Step 1 Go to the directory location of the error log file you specified during the import. (The default location and file name is **C:\Error.log**.)

Step 2 Use a text editor to open the error log file. You will use the error codes in the file to make corrections.

Step 3 Go to the directory location of the output log file you specified during the import. (The default location and file name is **C:\Output.log**.) This file contains all the records that were not imported.

Step 4 Use a text editor to open the output log file.

Step 5 Correct any records in the output file that are listed as errors in the error log file.

Step 6 When you have finished editing the output log file, save it as a CSV file with a new name.

Step 7 Run the Cisco Unity Bulk Import wizard again with the CSV file that you saved in Step 6.

Step 8 Repeat this procedure until all subscriber accounts are created without error, and then proceed to the "Issues to Consider After Creating Subscriber Accounts" section on page 21-28.

Using the Cisco Unity Administrator to Create Individual Subscriber Accounts

By using the Cisco Unity Administrator, you can create a regular subscriber account by either adding a new user to Active Directory or by importing existing user data from Exchange.

Adding Subscriber Accounts

If the subscriber that you want to create does not already have an Exchange mailbox, you can use the Cisco Unity Administrator to create an Exchange mailbox, an Active Directory domain account, and the new subscriber account at the same time. (If mailboxes for Cisco Unity subscribers will be homed in Exchange 2007, you do not have this option. You must create Active Directory accounts and Exchange mailboxes before you create Cisco Unity subscriber accounts.) Mailboxes are created on the server that you specified during Cisco Unity installation. Active Directory accounts are created in the domain and organizational unit (OU) that you specified during Cisco Unity installation.

Note In some cases, you may want the Active Directory accounts that Cisco Unity creates to be disabled. For more information, see the "How Cisco Unity Handles Active Directory Accounts for the Subscriber Accounts That You Create" section on page 21-5.

If you are not satisfied with this location, you can move the mailboxes as needed after the subscriber accounts have been created, or you can create the Active Directory account and Exchange mailbox first, and then use the Cisco Unity Administrator to import the user data into Cisco Unity. The user object created for the subscriber in Active Directory contains attributes specific to Cisco Unity.

Note that if a user already exists with the same alias as the subscriber that you want to create, the Cisco Unity Administrator notifies you that it cannot create the subscriber or the Exchange mailbox. This may happen if you choose to add a subscriber that already has an Exchange mailbox. To create the subscriber account in such cases, import the mailbox data for this user instead. You can use the Import Existing Exchange User option in the Cisco Unity Administrator to import the mailbox data for this user instead.

Note If you have not done so already, consider password security if you plan to create new Active Directory accounts at the same time that you create subscribers. See the "Ensuring That Subscribers Are Assigned Unique and Secure Active Directory Passwords" section on page 21-7 for details.

To create a regular Cisco Unity subscriber, do the procedure below.

To Create a Regular Subscriber Account by Adding a New User in Exchange

Step 1 In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page.

Step 2 Click the **Add** icon.

Step 3 Select **New Exchange Subscriber**.

Step 4 On the Add Subscriber page, enter the applicable information.

Step 5 Click **Add**.

Step 6 On the subscriber record, customize settings as applicable, and then click the **Save** icon.

Importing Existing User Data from the Message Store

If the subscriber that you want to create already has an Exchange mailbox, you can use the Cisco Unity Administrator to create a subscriber account by importing the mailbox data from Exchange. Cisco Unity-specific attributes are written to the existing directory user object when the subscriber is created.

When you use the Cisco Unity Administrator to import user data directly from the message store, Cisco Unity uses the mailbox data to create the Cisco Unity subscriber account. Cisco Unity does not enable Active Directory accounts if they are disabled at the time that you import mailbox data from Exchange.

This is important because subscribers whose Active Directory account is not enabled cannot access the Cisco Personal Communications Assistant (PCA) or the Cisco Unity Administrator, or use the phone as a recording and playback device for the Media Master. To avoid this problem, enable Active Directory accounts before you use the Cisco Unity Administrator to import data from the message store directory.

You can use the following procedure to import existing user data from Active Directory.

To Create a Regular Subscriber Account by Importing Existing User Data

Step 1 In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page.

Step 2 Click the **Add** icon.

Step 3 Select **Import Existing Exchange User**.

Step 4 Click **Select**.

Step 5 Select **Exchange**.

Step 6 In the Find By list, indicate whether to search by first name, last name, or Exchange alias. You can also indicate the domain for the search.

Step 7 Enter the applicable name or alias. You also can enter ***** to display a list of all users, or enter one or more characters followed by * to narrow your search.

Step 8 Click **Find**.

Step 9 On the list of matches, click the name of the user to import.

Step 10 On the Add Subscriber page, enter the applicable information.

Step 11 Click **Add**.

Step 12 On the subscriber record, customize settings as applicable, and then click the **Save** icon.

Using Integrated Mailbox Configuration to Create Individual Subscriber Accounts

When Cisco Unity is integrated with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) (version 4.1 or later), Cisco Unified CM administrators can create regular individual Cisco Unity subscriber accounts (referred to as voice mailboxes in Cisco Unified CM) from either the Directory Number Configuration page or the User Configuration page of the Cisco Unified Communications Manager Administration console. Cisco Unity subscriber accounts are then created directly in SQL by using browser-encrypted secure transmission of credentials across the network.

When subscriber accounts are created by using the Integrated Mailbox Configuration application, the accounts contain the minimum setup data that is provided by the Cisco Unity subscriber template that is chosen. If any customization of the subscriber account is necessary beyond what this template provides, you complete the customization by using the Cisco Unity Administrator. Note that after the accounts are created, there is no automatic synchronization of subscriber data between Cisco Unity and Cisco Unified CM. Any changes to subscriber accounts that exist in both systems, and that must be kept synchronized, will need to be made manually in both systems.

For information on setting up the Cisco Unity Cisco Unified CM Integrated Mailbox Configuration Wizard, or on using the Integrated Mailbox Configuration application, see the applicable *Cisco Unified Communications Manager Administration Guide* (available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html), and the Integrated Mailbox Configuration Help.

Issues to Consider After Creating Subscriber Accounts

After creating subscriber accounts, consider the following:

- Add individual subscribers to public distribution lists, as needed. For example, assign subscribers to screen those messages left in Cisco Unity that are not associated with a specific recipient, such as those left to the Unaddressed Messages distribution list or for the Opening Greeting call handler. See the "About Message Handling" section on page 8-3.
- If you are interested in preventing subscribers from appearing in the Outlook address book, see the "Preventing Subscribers from Appearing in Outlook Address Books" section on page 21-28.
- Set up the client applications that subscribers will use to access Cisco Unity from their computers. For details on setting up subscribers to use the Cisco PCA, the Cisco Unity Assistant, Cisco Unity Inbox, and ViewMail, see the "Setting Up Subscriber Workstations" chapter.
- Train new subscribers and operators to use Cisco Unity. See the "Subscriber Orientation" chapter for a task list you can use to acquaint subscribers with Cisco Unity.
- When a subscriber leaves the organization or otherwise no longer needs a Cisco Unity account, you can delete the subscriber account. See the "Deleting Subscriber Accounts" section on page 21-29.
- To modify subscriber accounts, see the "Modifying Subscriber Accounts" section on page 21-29.

Preventing Subscribers from Appearing in Outlook Address Books

Either before or after you create Cisco Unity subscriber accounts, you can prevent the subscribers from appearing in Outlook address books. In particular, you may wish to do so for Voice Messaging subscribers. For example, depending on your installation, the Voice Messaging subscribers may already have Active Directory accounts and Exchange mailboxes on your local network that they use for e-mail. Therefore, when Cisco Unity subscriber accounts are created for them, the Exchange address lists will contain duplicate listings—the existing user account that is used for e-mail and a new user account that is used only for voice mail. Both listings are included in the Outlook address book. This means that people may inadvertently send e-mail messages to the Voice Messaging account, which should be used only for addressing voice messages.

To discourage people from inadvertently sending e-mail messages to a Voice Messaging account, you can prevent subscribers from appearing in the Outlook address book altogether. When you prevent subscribers from appearing in Outlook address books, Exchange will still deliver e-mail messages addressed to them, but the number of messages may be reduced because other subscribers cannot use the Outlook address book to address messages to them. This can prevent the mailboxes of Voice Messaging subscribers from filling up with messages that they cannot access and delete.

To prevent subscribers from appearing in Outlook address books, you can use the Cisco Unity Administrator, the Cisco Unity Bulk Import wizard, Bulk Edit, or Active Directory Users and Computers:

- To do so in the Cisco Unity Administrator, uncheck the Show Subscriber in E-Mail Server Address Book check box on the Profile page for the subscriber template that you plan to use when creating subscribers, or on the Profile page for individual subscribers after you have created them.
- To do so by using the Cisco Unity Bulk Import wizard or the Bulk Edit utility, see the Help for each tool.
- To do so in Active Directory Users and Computers, click View > Advanced Features, double-click a recipient, and then check the Hide From Address Book check box on the Advanced tab.

Modifying Subscriber Accounts

If you want to change settings for multiple subscribers at once, there are two methods for you to choose from:

- Use the Bulk Edit utility to modify a subscriber setting that is shared by multiple subscriber accounts. For example, you might use this tool to change a setting so that a group of subscribers will no longer be listed in the phone directory, or to associate a group of subscribers with a particular class of service. Bulk Edit is available in the Tools Depot. (To access Tools Depot, double-click the Cisco Unity Tools Depot icon on the Cisco Unity server desktop. Note that not all subscriber settings are available for modification in Bulk Edit.)
- (Re)run the Cisco Unity Bulk Import wizard when you want to modify unique subscriber settings—such as phone passwords or extensions—for multiple subscribers at once. See Cisco Unity Bulk Import wizard Help. (To access the Cisco Unity Bulk Import wizard, on the Windows Start menu, click Programs > Cisco Unity > Cisco Unity Bulk Import. Note that not all subscriber settings are available for modification with the Cisco Unity Bulk Import wizard.)

If you want to change settings for an individual subscriber, you can also use the Cisco Unity Administrator.

Some of the settings that you enter on the subscriber pages of the Cisco Unity Administrator can also be changed by subscribers. Subscribers can customize some of their own settings either by accessing the Cisco Unity Assistant or by using the subscriber phone conversation.

Deleting Subscriber Accounts

Before deleting a regular subscriber account, review the following information:

- How to Delete a Subscriber Account, page 21-29
- What Happens When a Regular Subscriber Account Is Deleted, page 21-31

For information on deleting external subscriber accounts, see the following resources, as applicable:

- To delete AMIS subscriber accounts, see the “Deleting AMIS Subscribers” section in the “AMIS Networking” chapter in the *Networking Guide for Cisco Unity*.
- To delete Internet subscriber accounts, see the “Deleting Internet Subscribers” section in the “Internet Subscribers” chapter in the *Networking Guide for Cisco Unity*.
- To delete Bridge subscriber accounts, see the “Deleting Bridge Subscribers” section in the “About Bridge Networking” chapter in the *Networking Guide for Cisco Unity Bridge*.
- To delete VPIM subscriber accounts, see the “Deleting VPIM Subscribers” section in the “VPIM Networking” chapter in the *Networking Guide for Cisco Unity*.

The guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

How to Delete a Subscriber Account

When a subscriber leaves the organization or otherwise no longer needs a Cisco Unity account, delete the account in the Cisco Unity Administrator. It is important that you delete the subscriber account in the Cisco Unity Administrator before you delete the associated account in Active Directory, so that Cisco Unity can do the following tasks:

- Delete the subscriber from other Cisco Unity accounts, handlers, or call routing rules that send calls to the subscriber.
- Reassign to another subscriber (or distribution list) any call handlers that the subscriber owned or was the message recipient of.
- Reassign to another subscriber (or distribution list) any public distribution lists that the subscriber owned, and remove the subscriber from all public distribution lists.
- Reassign to a call handler any After Message Action, After Interview Action, or After Exit Action settings that were previously configured to send callers to the subscriber.

Cisco Unity reassigns these entities to the subscriber, distribution list, or call handler that is configured in the Substitute Objects fields on the System > Configuration > Settings page. By default, the Example Administrator is configured as the Substitute Recipient and Substitute Owner, and the Goodbye call handler is configured as the Substitute After Message Call Handler and Substitute Exit Call Handler. We recommend that you review the settings for these fields periodically, and update them if you wish to use different substitute objects, so that these entities can be properly reassigned any time a subscriber account is deleted.

Caution If you attempt to delete a subscriber account that is currently configured as a Substitute Owner or Substitute Recipient, you will be warned that the subscriber is currently being used as a substitute value, and that you should select another substitute before continuing with the deletion. Likewise, if you attempt to delete a subscriber account when any of the substitute object values are empty (because you have previously deleted the subscriber or call handler that was configured as a substitute), you will be warned that one or more substitute objects has not been configured, and you will be asked whether you want to continue with the deletion. In both cases, you are allowed to ignore the warnings and continue with the deletion of the subscriber account, even when the subscriber account is the owner or recipient of entities in Cisco Unity. If you continue with the deletion, the result can be corruption of the Cisco Unity database.

When you delete a subscriber who was assigned to review the messages sent to any of the following Cisco Unity entities, make sure that you assign another subscriber or a public distribution list to replace the deleted subscriber; otherwise, messages may be lost.

- Unaddressed Messages distribution list (because the Example Administrator is by default the only member of this distribution list)
- System Event Messages distribution list (because the Example Administrator is by default the only member of this distribution list)
- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

To identify call handlers that are associated with improperly deleted accounts, run the Unresolved References report. See the “Unresolved References Report” section in the “Reports” chapter of the *Maintenance Guide for Cisco Unity* for more information. The *Maintenance Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Use the following procedure to delete a subscriber account in the Cisco Unity Administrator.

To Delete a Subscriber Account

Step 1 In the Cisco Unity Administrator, go to the **System > Configuration > Settings** page.

Step 2 Confirm that Substitute Objects are assigned appropriately. If the subscriber account you are going to delete is listed in any of the fields as a Substitute Object, reassign the value to another subscriber or distribution list.

Step 3 Go to any **Subscribers > Subscribers** page, and search for the subscriber account that you are going to delete. (For detailed instructions on searching for a subscriber account, see the "To Find a Subscriber Record" procedure on page 1-11.)

Step 4 From the subscriber page, click the **Delete** icon.

Step 5 Click **Delete**.

What Happens When a Regular Subscriber Account Is Deleted

When you delete a Cisco Unity subscriber account, Cisco Unity removes all data associated with the subscriber account from a SQL Server database on the Cisco Unity server.

In addition, Cisco Unity removes the small subset of subscriber account information that is stored in Active Directory.

Note that deleting the Cisco Unity account does not delete the Active Directory account (if there is one) or the Exchange mailbox for that subscriber. As needed, the Active Directory account can be deleted separately after the subscriber account is deleted in the Cisco Unity Administrator.

The Bulk Subscriber Delete tool in the Cisco Unity Tools Depot can be used to delete multiple subscriber accounts. The tool also includes the option to delete the associated Active Directory accounts and mark the Exchange mailboxes for deletion. Read the Help file carefully before using this tool.

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

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: • 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.)

CHAPTER 23

Setting Up Message Notifications

See the following sections in this chapter:

Message Notifications Overview

Message notification settings allow you to control how and when Cisco Unity notifies a subscriber of new messages. Cisco Unity can notify a subscriber of new messages by calling a phone or pager, or by sending an e-mail. Additionally, Cisco Unity can send message notifications in the form of text messages to text pagers and text-compatible cell phones using SMTP or in the form of SMS messages to wireless devices using SMPP.

Note that any message notification that you set up on the Subscribers > Subscribers > Message Notification page is in addition to the message waiting indication (MWI) that you set up on the Subscribers > Subscribers > Messages page.

By default, if Cisco Unity sends a notification of a new message to a device (such as a cell phone) and the device forwards the call back to Cisco Unity because the device did not answer, Cisco Unity will reject the forwarded message notification call. As a result, the subscriber mailbox will not be filled with forwarded message notification announcements. Because Cisco Unity rejects the forwarded message notification call, the call does not create a new message for the subscriber and does not trigger a new message notification call.

To set up message notification for a subscriber, you select a notification device—phone, pager, text pager, or SMS (SMPP) device—and enter a phone number or e-mail address, as applicable. (Before you can set up SMTP or SMS (SMPP) notifications, you must first set up an SMTP gateway and/or enter the SMPP provider information, as applicable for each. For details, see the "Setting Up Text Message Notifications" section on page 23-2.) The settings for each notification device allow you to control when and how notifications are sent to the first and subsequent devices. Generally, you adjust these settings on the message notification page of a specific subscriber and not in the subscriber template. However, you may want to enter notification settings in the subscriber template if, for example, you want to set up "chaining" or "cascading" message notification for an entire department of new subscribers. For setup instructions, see the "Setting Up Chaining Message Notification" section on page 23-6, and the "Setting Up Cascading Message Notification" section on page 23-7.

Subscribers can set up message notification themselves by using the Cisco Unity Assistant, if available. Subscribers can also enter the phone number and status for four of the notification devices—home phone, work phone, spare phone, and pager—by using Cisco Unity phone menus.

Setting Up Text Message Notifications

Cisco Unity can send message notifications in the form of text messages to text pagers, text-compatible cell phones, and e-mail addresses. When a message arrives that matches the criteria selected in the message notification settings, the Cisco Unity Messaging System sends a text message entered by you or the subscriber, such as "Urgent message for Technical Support."

There are three types of text message notifications available with Cisco Unity. See the following sections for a summary of each type, and information on what you need to do before you can enable text message notifications for subscribers or offer them as options that subscribers can set up themselves in the Cisco Unity Assistant.

- SMTP Message Notifications, page 23-2
- SMS (SMPP) Message Notifications, page 23-3
- Cisco Unity Inbox Message Notifications, page 23-4

SMTP Message Notifications

By using SMTP, Cisco Unity can send text message notifications to text pagers that support SMTP when subscribers have received a new voice, e-mail, or fax message. Cisco Unity can also use SMTP to send a text message notification to an e-mail address. This is especially useful when subscribers use text-compatible cell phones or other devices that have been assigned an SMTP address by their wireless or mobile service provider.

In order for subscribers to receive SMTP message notifications from Cisco Unity, your site must have an SMTP gateway. When the gateway is set up, you can use the Text Pager 1 or Text Pager 2 options on the Subscribers > Subscribers > Message Notification page to enable Cisco Unity to send text message notifications by using SMTP. Alternatively, subscribers can enable the same devices on the Notification Devices page in the Cisco Unity Assistant.

Note that when a site without an SMTP gateway attempts to deliver text message notifications, the notification attempt fails and a nondelivery receipt (NDR) is sent to the Cisco Unity Messaging System and then routed, by default, to the Unaddressed Messages distribution list. (For more information, see the "How Cisco Unity Handles Messages Without a Specific Recipient" section on page 8-6.)

If the service provider that most subscribers use for their cell phones or other devices simply convert incoming SMTP message notifications to SMS messages, consider using SMS (SMPP) message notifications instead. The "SMS (SMPP) Message Notifications" section on page 23-3 details the advantages of using SMS messaging.

Tip If you specify that Cisco Unity provides caller information in the notifications, consider that subscribers may not wish to hear the information again when they log on to Cisco Unity by phone to play the message. You can use the Custom Key Map utility to map a key (for example, the # key) so that subscribers can easily skip from the message header to the message body. (You assign subscribers to a Custom Keypad Mapping conversation on the Subscribers > Subscriber > Conversation page in the

Cisco Unity Administrator. For information on using the utility, see Custom Key Map utility Help.) Alternatively, subscribers can use the Cisco Unity Assistant to specify that Cisco Unity does not play caller information before playing messages.

SMS (SMPP) Message Notifications

With the services and information provided by a wireless carrier, mobile messaging service provider or similar company, Cisco Unity can use the Short Message Peer-To-Peer (SMPP) protocol to send message notifications in the Short Message Service (SMS) format to GSM cell phones and other SMS-compatible devices when subscribers receive a new voice, e-mail, or fax message. SMS is a "store and forward service," which means that messages are not sent directly to the device used by the message recipient. Instead, an application like Cisco Unity—known as an External Short Message Entity (ESME)—submits a message to the SMS Center (SMSC). The SMSC then forwards the message to the device.

Advantages Over SMTP Message Notifications

An advantage of using SMS is that the subscriber device receives message notifications much faster than when using SMTP. The subscriber device does not have to be on the GSM network at the time that Cisco Unity sends the message to the SMSC, nor when the SMSC forwards it. The GSM network holds the SMS messages until the device is available; when the device is available, the delivery of the queued messages to the device takes just a few seconds. In addition, you can configure Cisco Unity so that each notification message replaces the previous one. Note that this functionality may not be supported by all mobile service providers.

SMS Message Length Limitations

An SMS message is a short text message. The acceptable message length for an SMS message varies depending on the service provider, the character set used to compose the message text, and the specific characters used in the message text. In general, you can use the following table to determine how long SMS messages can be:

Character Set	Message Length Limitation
7-bit	160 alphanumeric characters
8-bit	140 alphanumeric characters
16-bit	70 alphanumeric characters

Because Cisco Unity supports all three of the above character sets, the Cisco Unity Administrator and the Cisco Unity Assistant allow subscribers to enter up to 160 characters of message text. However, depending on the character set you configure Cisco Unity to use, messages that are shorter than 160 characters may be truncated. The text of the message and the message count (assuming subscribers choose to include the message count) constitute total message length.

Cost Considerations

When setting up SMS (SMPP) message notifications, consider that service providers typically charge for each SMS message or group of messages sent. Thus, the more SMS (SMPP) message notifications that Cisco Unity sends to subscriber devices, the higher the costs to your organization. For this reason, you may want to restrict the use of this feature to a group of subscribers (you can do so by assigning owners to the SMPP providers that you create on the System > SMPP Provider page), or you may want to ask subscribers to limit the number of message notifications that they receive by message type or

urgency. For example, subscribers can specify in the Cisco Unity Assistant that Cisco Unity will send message notifications only when new voice messages arrive, or only when a new voice or urgent e-mail message arrives, and so on.

Task List for Setting Up SMS (SMPP) Message Notification

To enable SMS (SMPP) message notifications for subscribers with SMS-compatible devices, do the following tasks:

1. Set up an account with a mobile messaging service providers that offers SMS messaging. Cisco Unity works with any service provider that supports the SMPP version 3.3 or SMPP version 3.4 protocols.
2. Gather the information needed to allow Cisco Unity to communicate with the SMPP server at the SMSC affiliated with your contracted service provider, and enter the information on the System > SMPP Provider page.

   For example, you will need to know the SMPP server name, TCP port, account name and password, and other similar information, as indicated in the documentation that your service provider gave you on setting up a messaging server to communicate with an SMSC. See the "Setting Up an SMPP Provider" section on page 23-5 for additional details and procedures.
3. When the Cisco Unity server is set up behind a firewall, configure the TCP port that is used by the SMPP server to connect to Cisco Unity to allow incoming and outgoing communication between Cisco Unity and the SMPP server.
4. Set up SMS (SMPP) message notification for yourself or another willing subscriber, and test to see if the device receives the SMS (SMPP) notification as expected. If notifications are not working, confirm that you entered the settings on the System > SMPP Provider page as indicated in the documentation that your service provider gave you. Contact your service provider for assistance, as needed.
5. Enable the SMS (SMPP) message notification for applicable subscriber accounts. Subscribers can also set it up for themselves in the Cisco Unity Assistant.

Note that while neither the Cisco Unity Bulk Import wizard nor the Bulk Edit utility (available in Tools Depot) allow you to enable SMS (SMPP) message notifications, you can use the Bulk Edit utility to disable SMS (SMPP) notifications at any time for multiple subscribers at once. For logging and troubleshooting information, see the "Message Notification" chapter of the *Troubleshooting Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.

Cisco Unity Inbox Message Notifications

You can also set up a text message notification so that subscribers receive an e-mail notification in their respective e-mail Inboxes when a new voice message arrives in their Cisco Unity Inbox. With Cisco Unity Inbox notifications, you can also enter the URL for the Cisco PCA on the System > Configuration page so that it is automatically included as a link in the body of the e-mail message that is sent to the subscriber.

Consider setting up Cisco Unity Inbox notifications for Voice Messaging subscribers who work remotely and have e-mail access. These subscribers rely on MWIs on their desk phones to tell them when a new message arrives when they are in the office. When they work remotely, they may appreciate the convenience of Cisco Unity Inbox notifications so that they do not need to call Cisco Unity periodically to check for new messages.

In order for subscribers to receive Cisco Unity Inbox message notifications, your site must have an SMTP gateway. When the gateway is set up, you can use the Text for Cisco Unity Inbox option on the Subscribers > Subscribers > Message Notification page to enable Cisco Unity Inbox message notifications for subscribers. Alternatively, subscribers can enable it on the Notification Devices page in the Cisco Unity Assistant.

Note that when a site without an SMTP gateway attempts to deliver text message notifications, the notification attempt fails and a nondelivery receipt (NDR) is sent to the Cisco Unity Messaging System and then routed, by default, to the Unaddressed Messages distribution list. (For more information, see the "How Cisco Unity Handles Messages Without a Specific Recipient" section on page 8-6.)

Setting Up an SMPP Provider

Before you can offer SMS (SMPP) message notifications to subscribers, you must set up Cisco Unity so that it can communicate with the SMS Center (SMSC) that is affiliated with the mobile messaging service provider(s) that your organization has contracted with to provide SMS messaging services.

When you have an account, the service provider sends you the information necessary to configure an application like Cisco Unity—known as an External Short Message Entity (ESME)—to use the SMPP protocol to send text messages to the SMPP server at the SMSC. Then you enter the information on the System > SMPP Provider page.

Use the procedures in this section to create and modify SMPP providers. You can create as many SMPP providers as you need. The providers that you add are available to all subscribers to use for SMS (SMPP) message notifications unless you specify otherwise. Consider that the more SMS (SMPP) message notifications that Cisco Unity sends to subscriber devices, the higher the costs to your organization (depending on the account, service providers typically charge for each SMS message or group of messages). For this reason, you may want to restrict the use of this feature to a group of subscribers by assigning owner(s) to the SMPP provider(s) that you create.

Note When the Cisco Unity server is set up behind a firewall, configure the TCP port that is used by the SMPP server to connect to Cisco Unity to allow incoming and outgoing communication between Cisco Unity and the SMPP server.

For a general overview of how SMS (SMPP) message notifications work, see the "SMS (SMPP) Message Notifications" section on page 23-3. Subscribers can also set up SMS (SMPP) message notifications for themselves in the Cisco Unity Assistant.

To Create an SMPP Provider

Step 1 In the Cisco Unity Administrator, on the **System > SMPP Provider** page, click the **Add** icon.

Step 2 In the Add SMPP Provider dialog box, in the Provider Name field, enter the name that you want to represent the service provider in Cisco Unity applications.

The name you enter here will be listed on the Provider SMPP lists displayed on the SMS (SMPP) message notification pages for subscribers and subscriber templates in the Cisco Unity Administrator, as well as in the Cisco Unity Assistant.

Step 3 Do one of the following:

- To allow all subscribers to use this provider, skip to Step 4.

- To restrict provider use to a particular subscriber, click the **Assign** button. Then, select the applicable subscriber from the list. (Note that once you save the provider, the owner is not displayed in the Cisco Unity Administrator. For this reason, consider naming a provider accordingly when you assign one to a particular subscriber.)

Step 4 For the remainder of the page, enter information as applicable in the fields provided. Depending on the SMSC used by your service provider(s), you may not need to complete every field. To determine which fields are required, see the documentation on setting up a messaging server to communicate with the SMSC that your service provider sent you.

Tip Field Help definitions in the Cisco Unity Administrator also include additional information about the fields on the page.

Step 5 For multilingual systems, consider adding an SMPP provider for each language that subscribers use and then name and configure the providers accordingly. (Use the Data Coding field to specify language preference.)

Step 6 Click the **Save** icon.

To Modify an SMPP Provider

Step 1 In the Cisco Unity Administrator, go to any **System > SMPP Provider** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the SMPP Provider that you want to modify. (Note that you cannot modify provider ownership.)

Step 4 Change settings as applicable, and then click the **Save** icon.

Depending on the SMSC used by your service provider(s), you may not need to complete every field on the System > SMPP Provider Settings page. To determine which fields are required, see the documentation on setting up a messaging server to communicate with an SMSC that your service provider sent you. For technical details about the SMPP protocol, review the SMPP Protocol Specification for the applicable SMPP version you configure Cisco Unity to use. The document is available on the Internet.

Setting Up Chaining Message Notification

Message notification can be set to "chain" to a series of notification devices if an attempt to send notification to the first selected device fails. The definition of failure to a notification device is based on the options you select for retrying a device that is not answered or is busy.

The Cisco Unity Administrator does not allow pager devices to be used for chaining message notification because notification to these devices does not fail.

To Set Up Chaining Message Notification

Step 1 In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page.

Step 2 Click a notification device from the Device list, and enter settings for it, as applicable.

Step 3 Click another device in the If Notification Fails, Send Notification To field.

Step 4 In the Device list at the top of the page, click the same device that you indicated in Step 3, and enter settings for it as you would normally, with the following exceptions:

- In the Notify Subscriber Of table, uncheck all types and urgency of messages that should generate notification. If any message types are checked in this table, message notification for this device will commence immediately and will not wait for the notification failure of the previous device. Therefore, your notifications will not chain but all trigger at once.
- In the Send Initial Notification After How Many Minutes field, leave the default setting of **0**.

Step 5 Repeat Step 3 and Step 4 for any subsequent devices that you wish to chain for message notification.

Setting Up Cascading Message Notification

Cascading message notification allows you to set up a series of notifications to a widening circle of recipients. Cisco Unity continues to send notifications according to the devices you selected until the message has been saved or deleted by a recipient.

For example, to create a cascade of message notifications for your Technical Support department, set the first message notification to be sent immediately to the pager of the front-line technical support representative. If the first notification has not be saved or deleted after a delay of 15 minutes, the next notification can be sent to the pager of the department manager. A third notification can be set up to call an employee in the Problem Resolution Group if the second notification is not saved or deleted after 30 minutes, and so on.

To Set Up Cascading Message Notification

Step 1 In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Message Notification** page.

Step 2 On the Notification Device page, select a notification device and enter the applicable settings so that it notifies a person in the recipient list for the cascading notification. For example, for the first recipient, you would enter the phone number for the pager that belongs to the front-line technical support representative.

Step 3 In the Send Initial Notification After How Many Minutes? field, enter the desired delay for the device, in minutes.

Space notifications between each device at regular intervals, such as every 15 minutes. For the first device you set up, consider specifying 0 as the delay so that the first recipient receives the notification immediately. For the device of the second recipient, specify 15 minutes. Specify 30 minutes for the device of the next recipient, and so on.

Step 4 Select **None** in the If Notification Fails, Send Notification To field.

Step 5 Click **Save**.

Step 6 Repeat Step 2 through Step 5 to set up another device for the next person on the recipient list for the cascading notification.

CHAPTER 24

Setting Up Broadcast Messaging

System broadcast messages are recorded announcements that are sent to everyone in an organization (or to particular location(s) within an organization). You determine whether subscribers can use the Cisco Unity Broadcast Message Administrator to send and/or update broadcast messages. (By default, Cisco Unity subscribers are not enabled to use the Cisco Unity Broadcast Message Administrator.)

See the following sections in this chapter:

System Broadcast Messages Overview

Though system broadcast messages may sound similar to regular voice messages, they are not simply voice messages sent to a large distribution list. A system broadcast message is unique in the following ways:

- System broadcast messages are played immediately after subscribers log on to Cisco Unity by phone—even before they hear message counts for new and saved messages. After logging on, subscribers hear how many system broadcast messages they have and Cisco Unity begins playing them.
- For each system broadcast message, the sender specifies how long Cisco Unity will broadcast the message. The sender can specify that a system broadcast message is “active” for a day, a week, a month—even indefinitely. Subscribers hear only the system broadcast messages that are active at the time that they log on to Cisco Unity.
- Subscribers must listen to each system broadcast message in its entirety before Cisco Unity allows them to hear new and saved messages or to change setup options. Subscribers cannot fast-forward or skip a system broadcast message.
- If a subscriber hangs up before playing the entire system broadcast message, the message plays again the next time that the subscriber logs on to Cisco Unity by phone (assuming that the message is still active).

- When a subscriber has finished playing a system broadcast message, the message can either be replayed or permanently deleted. Subscribers cannot respond to, forward, or save system broadcast messages.
- Subscribers can receive an unlimited number of system broadcast messages.
- Subscribers receive system broadcast messages even when they exceed their mailbox size limits and are no longer able to receive other messages. Because of the way that the messages are stored on the Cisco Unity server, they are not included in the total mailbox size for each subscriber.
- New subscribers hear all active broadcast messages immediately after they enroll as a Cisco Unity subscriber.
- System broadcast messages do not light message waiting indicators (MWIs) on subscriber phones, nor do they cause distinctive dial tones to notify subscribers of a new message when they pick up their desk phone receiver. System broadcast messages also do not trigger message notifications for alternative devices, such as a pager or another phone.
- Subscribers do not receive system broadcast messages in the Cisco Unity Inbox.
- Unified Messaging subscribers do not receive system broadcast messages in their e-mail Inboxes.

It is important to note that when a system broadcast message is sent to a public distribution list that contains Internet, AMIS, Bridge, or VPIM subscribers in addition to regular Cisco Unity subscribers, the message is delivered to all recipients on the list as a regular voice message—not a system broadcast message. Thus, none of the characteristics listed above apply, and MWIs are triggered, subscribers can skip the message, the message will appear in the Cisco Unity Inbox and e-mail Inboxes, and so on.

To prevent this from happening, set up public distribution lists that include VPIM subscribers to represent each location where subscribers should receive the message, and use these lists when you send system broadcast messages to subscribers on multiple servers in the network. A similar approach can also be used to include subscribers on a Cisco Unity Express server in the distribution of a system broadcast message.

Task List for Setting Up and Offering Access to the Cisco Unity Broadcast Message Administrator

Use the following task list to set up broadcast messaging:

1. Set up the Cisco Unity Broadcast Message Administrator on each Cisco Unity server. See the "Setting Up the Cisco Unity Broadcast Message Administrator" section on page 24-3.
2. *(Optional)* Use the Advanced Settings tool on each Cisco Unity server to specify:
   - Maximum recording length of system broadcast messages. By default, subscribers can record messages up to 3,600,000 milliseconds (60 minutes) in length. The setting is called Conversation—System Broadcast Message Maximum Recording Length.
   - The order in which Cisco Unity presents system broadcast messages to subscribers. By default, the oldest messages play first. The setting is called Conversation—System Broadcast Message Playback Order.
   - How long Cisco Unity retains expired system broadcast messages on the server. By default, Cisco Unity purges the WAV file and any data associated with a message 30 days after its end date and time. The setting is called Conversation—System Broadcast Message Retention Period.

- The number of days that a system broadcast message remains active when the subscriber does not specify an end date and time. The default is 30 days. The setting is called Conversation—System Broadcast Message Default Active Days.
- How often Cisco Unity checks for new system broadcast messages. By default, Cisco Unity checks for new messages every five minutes. The setting is called Conversation—System Broadcast Message Check Frequency.

See Advanced Settings Help for details on each setting. (The Advanced Settings tool is available in Tools Depot.)

3. Enable subscribers to send system broadcast messages. See the "Enabling Subscribers to Send and Update System Broadcast Messages" section on page 24-4.
4. If applicable, set up distribution list(s) so subscribers can use the Cisco Unity Broadcast Message Administrator to send broadcast messages to VPIM locations.

   To do so, you first must understand how broadcast messaging works with networked servers. See the "Networked System Broadcast Messages" section in the "Using VPIM for Networking with Cisco Unity Express or Other Cisco Unity Systems" chapter of the *Networking Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
5. Let the applicable subscribers know how to access and use the two tools for sending and managing system broadcast messages. See the "Using the Cisco Unity Broadcast Message Administrator and the Cisco Unity Broadcast Message Administrator Tool to Send and Manage System Broadcast Messages" section on page 24-6.

   Make sure that those who are able to send system broadcast messages to subscribers on multiple servers understand the meaning of each addressing option offered by the Cisco Unity Broadcast Message Administrator, and that they understand how to address a message to reach subscribers on a particular group of servers.

   See the applicable section in the *Networking Guide for Cisco Unity*:

   - The "Addressing System Broadcast Messages to Digitally Networked Servers" section in the "Digital Networking" chapter.
   - The "Addressing System Broadcast Messages to Multiple Servers" section in the "Using VPIM for Networking with Cisco Unity Express or Other Cisco Unity Systems" chapter.

   The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Setting Up the Cisco Unity Broadcast Message Administrator

To send a system broadcast message, Cisco Unity subscribers log on to the Cisco Unity Broadcast Message Administrator—a special conversation that allows them to send and/or update system broadcast messages. You can give subscribers access to the Cisco Unity Broadcast Message Administrator in one of the following ways:

- **Create a call handler to send subscribers to the Cisco Unity Broadcast Message Administrator**—You can create a new call handler, assign it a unique extension, and specify that Cisco Unity sends the subscriber to the Broadcast Message Administrator as the after-greeting action. To make the transfer quick and seamless to subscribers, select a blank greeting for the call handler.

See the "Creating and Modifying Call Handlers" section on page 4-2 for instructions.

- **Set up a Custom Keypad Mapping conversation that maps a key to the Broadcast Message Administrator and offers it to subscribers in the main menu**—By using the Custom Key Map utility, you can add the Broadcast Message Administrator to the options offered to subscribers at the main menu. Then, configure subscriber accounts to use the Custom Keypad Mapping conversation.

  See the "Using the Custom Keypad Mapping Utility to Customize the Conversation" section on page 14-15 for instructions.

- **Offer the Cisco Unity Broadcast Message Administrator as a one-key dialing option from a greeting**—You can specify that Cisco Unity will send a caller to the Broadcast Message Administrator (on the Caller Input page for any call handler or subscriber greeting) when a caller presses a particular key during the greeting. For example, you could specify that Cisco Unity sends the caller to the Cisco Unity Broadcast Message Administrator when a subscriber presses a particular key during the Opening Greeting or even during his or her own greeting.

  To set up a one-key dialing option for accessing the Cisco Unity Broadcast Message Administrator, use caller input settings for a call handler to send callers to the Broadcast Message Administrator conversation when they press the key that you specify during a call handler greeting. Then, enable caller input for the applicable greeting. Optionally, you can (re)record the greeting to mention the key that callers can press in the call handler greeting. (For example, "...for the Cisco Unity Broadcast Message Administrator, press 3.")

- **Set up a special "Cisco Unity Broadcast Message Administrator" phone number and routing rule**—See the documentation for the phone system to set up a new phone number. Then, on the Call Management > Call Routing > Direct Calls page in the Cisco Unity Administrator, create a routing rule that sends any call that arrives for the new number to the Broadcast Message Administrator conversation. Distribute the new number to callers who are enabled to send and/or update system broadcast messages.

  For additional information on setting up call routing rules, see the "Creating and Modifying Call Routing Rules" section on page 3-5.

Enabling Subscribers to Send and Update System Broadcast Messages

Because system broadcast messages are designed to convey important and often time-sensitive information to a large number of subscribers at once, Cisco Unity subscribers can use the Cisco Unity Broadcast Message Administrator only if they are enabled to do so in the Cisco Unity Administrator. By default, Cisco Unity subscribers are not enabled to use the Cisco Unity Broadcast Message Administrator to send or update system broadcast messages.

In the Cisco Unity Administrator, you can specify whether subscriber(s) can send system broadcast messages to all subscribers on the local Cisco Unity server, to all locations in the Cisco Unity global directory, or to specific locations and/or public distribution lists set up for system broadcast messaging to remote networks. You can also specify whether subscribers can update system broadcast messages stored on the local Cisco Unity server. If you want to enable an existing group of subscribers to send system broadcast messages, you can use the Bulk Edit tool available in Tools Depot.

Consider how subscribers in your organization might use system broadcast messaging when determining which Cisco Unity subscribers can send and update system broadcast messages, and whether they can send messages to subscribers on the local Cisco Unity server, or other locations and/or remote networks. For example, as a Cisco Unity administrator, you may want to send a welcome message to subscribers on a new system or remind all Cisco Unity subscribers to change their phone passwords. You may also

want to use system broadcast messages as a way to train subscribers on how to use Cisco Unity features or to summarize changes to Cisco Unity after an upgrade. Other Cisco Unity subscribers—such as network administrators, members of management, Human Resources personnel, and facilities managers—may also need to send system broadcast messages to announce planned network outages for particular locations, organization-wide goals and personnel changes, branch office closures for holidays, security alerts, and the like.

You can use the following procedures to enable subscribers to send and update system broadcast messages:

- Do the "To Enable Sending and Updating System Broadcast Messages in a Subscriber Template" procedure on page 24-5 to allow a group of subscribers to send and update system broadcast messages. (Keep in mind that changes to settings in a template do not affect any of the existing subscriber accounts that were based on that template; your updates to the template settings will affect only those subscribers whose accounts are created after you make the updates.)
- Do the "To Enable an Existing Subscriber to Send and Update System Broadcast Messages" procedure on page 24-6 to allow an existing subscriber to send and update system broadcast messages. Alternatively, you can use the Bulk Edit utility in Tools Depot to modify multiple subscriber accounts at once. See Bulk Edit utility Help for details.

To Enable Sending and Updating System Broadcast Messages in a Subscriber Template

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Template** page, and find the template that you want to modify.

Step 2 Browse to the **Features** page.

Step 3 Under Broadcast Messages, check the applicable check boxes:

- **Subscriber Can Send Broadcast Messages to Subscribers on This Server**—Check this check box to allow subscribers to send system broadcast messages to all subscribers on the local Cisco Unity server.
- **Subscriber Can Send Broadcast Messages to Subscribers on Multiple Servers**—Check this check box to allow subscribers to send system broadcast messages to all locations in the Cisco Unity global directory, or to specific locations and/or public distribution lists set up for system broadcast messaging. (By checking this check box, you also enable subscribers to send broadcast messages to all subscribers on the local Cisco Unity server.)
- **Subscriber Can Update Broadcast Messages Stored on This Server**—Check this check box to allow subscribers to edit system broadcast messages stored on the local Cisco Unity server. Note that by checking this check box, you also enable subscribers to send system broadcast messages to all subscribers on the local Cisco Unity server.

  Consider that when a system broadcast message is sent to multiple locations, a copy of the message is sent to each server and then distributed to the subscribers homed on that server. As a result, subscribers must make updates to each message locally. To do so, subscribers must be enabled to update messages on each server and then they must log on to Cisco Unity Broadcast Message Administrator for each Cisco Unity server to update the messages.

Step 4 Click the **Save** icon.

To Enable an Existing Subscriber to Send and Update System Broadcast Messages

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page and find the applicable subscriber.

Step 2 Browse to the **Features** page.

Step 3 Under Broadcast Messages, check the applicable check boxes:

- **Subscriber Can Send Broadcast Messages to Subscribers on This Server**—Check this check box to allow subscribers to send broadcast messages to all subscribers on the local Cisco Unity server.
- **Subscriber Can Send Broadcast Messages to Subscribers on Multiple Servers**—Check this check box to allow subscribers to send system broadcast messages to the local Cisco Unity server, to all locations in the Cisco Unity global directory, or to specific locations and/or public distribution lists set up for broadcast messaging. (By checking this check box, you also enable subscribers to send broadcast messages to all subscribers on the local Cisco Unity server.)
- **Subscriber Can Update Broadcast Messages Stored on This Server**—Check this check box to allow subscribers to edit system broadcast messages stored on the local Cisco Unity server. Note that by checking this check box, you also enable subscribers to send system broadcast messages to all subscribers on the local Cisco Unity server.

  Consider that when a system broadcast message is sent to multiple locations, a copy of the message is sent to each server and then distributed to the subscribers homed on that server. As a result, subscribers must make updates to each message locally. To do so, subscribers must be enabled to update messages on each server and then they must log on to Cisco Unity Broadcast Message Administrator for each Cisco Unity server to update the messages.

Step 4 Click the **Save** icon.

Using the Cisco Unity Broadcast Message Administrator and the Cisco Unity Broadcast Message Administrator Tool to Send and Manage System Broadcast Messages

This section details how to use the Cisco Unity Broadcast Message Administrator—a special conversation that allows you to send and manage broadcast messages by phone, and the Broadcast Message Administrator Tool—a tool with a graphical interface that allows you to send and manage system broadcast messages for the local Cisco Unity server.

See the following sections:

- About the Cisco Unity Broadcast Message Administrator, page 24-7
- About the Cisco Unity Broadcast Message Administrator Tool, page 24-7

About the Cisco Unity Broadcast Message Administrator

Subscribers who are able to send system broadcast messages can use the Cisco Unity Broadcast Message Administrator to do the following tasks:

- Record and send one or more system broadcast messages. If the subscriber hangs up or is disconnected before sending the system broadcast message(s), Cisco Unity deletes the recording(s).
- Define when a system broadcast message becomes active and for how long. Unless otherwise specified by the subscriber, each message is set to broadcast immediately and to remain active for 30 days. Subscribers can set a future date and time for the message to be broadcast up to one year in advance, and can specify that a system broadcast message is "active" for a day, a week, a month—even indefinitely. (Date and times reflect the time zone for the subscriber who sends the message, not those who receive it.)

Note If the delivery of a system broadcast message fails, the subscriber who sent it will receive a nondelivery receipt (NDR), indicating that the delivery failed and if known, the reason why it failed. However, unlike the process of sending other voice messages, the subscriber cannot resend the system broadcast message after playing the NDR. Instead, the subscriber must log on to the Cisco Unity Broadcast Message Administrator to re-record the message and send it again.

Subscribers who are able to update system broadcast messages can use the Cisco Unity Broadcast Message Administrator to do the following tasks on the local Cisco Unity server:

- Review active messages. (If there is more than one active message, the Cisco Unity Broadcast Message Administrator presents them in order based on the start date and time, starting with the newest messages.)
- Change the end date and time for active messages.
- Change or add to a recording for future messages. (Note that Cisco Unity enforces the total message length limit even when material is added to a message.)
- Change the start date and time and/or the end date and time for future messages. (Note that the end date and time does not adjust automatically if subscribers change the start date and time but do not change the end date and time.)
- Delete active and future messages. (Note that Cisco Unity does not report which subscribers have already played an active message.)

About the Cisco Unity Broadcast Message Administrator Tool

The graphical interface for the Broadcast Message Administrator Tool offers an easy way to specify the recording and schedule for a new system broadcast message, to play active system broadcast messages and review who has played them, and to delete system broadcast messages. Although no class of service rights are required to use the tool, administrators must be able to log on to the Cisco Unity server to use it.

The tool is available in Tools Depot. To learn how to use it, see Broadcast Message Administrator Tool Help.

CHAPTER 25

Managing Distribution Lists

See the following sections in this chapter:

Public Distribution Lists Overview

Public distribution lists are used to send voice messages to multiple subscribers. The subscribers that are assigned to a public distribution list typically are subscribers who need the same information on a regular basis, such as employees in a department or members of a team. The class of service that is associated with each subscriber account dictates whether subscribers can send messages to public distribution lists in Cisco Unity.

Predefined Public Distribution Lists

Cisco Unity includes the following predefined public distribution lists, which you can modify but not delete:

All Subscribers	By default, the All Subscribers list is included in the {Default Subscriber} template. When subscriber accounts are created, they are automatically added to this list.

Unaddressed Messages	Subscribers who are assigned to the Unaddressed Messages list receive messages left in the Operator call handler when the operator is not available. Additionally, when the Cisco Unity Messaging System receives a nondelivery receipt (NDR) for a voice message—because, for example, an unidentified caller leaves a message for a subscriber whose mailbox is full—it is forwarded to the Unaddressed Messages list. When Cisco Unity is installed, the Example Administrator account is set as the only member of the Unaddressed Messages and System Event Messages distribution lists. Do not delete the Example Administrator account unless you have assigned the applicable subscriber(s) or another distribution list to review the messages sent to these two distribution lists. In addition, note that if you later delete the assigned subscribers or distribution lists, Cisco Unity does not prompt you to assign a replacement. Finally, note that if the mailbox(es) of the subscriber(s) who are assigned to check the Unaddressed Messages list are full, the messages are lost. For more information, see the "How Cisco Unity Handles Full Mailboxes" section on page 8-4.

In each subscriber template, you can specify the public distribution lists to which each new subscriber based on that template will be added. You can also add individual subscribers directly to the public distribution lists. When you delete a subscriber account, Cisco Unity automatically removes the subscriber from any public distribution list of which the subscriber is a member.

Creating and Modifying Public Distribution Lists

You can modify the predefined lists, and you can create new ones. Additionally, you can import public distribution lists from Exchange. Both Cisco Unity subscribers and non-subscribers are included as members of an imported distribution list, though non-subscribers are not displayed in the Cisco Unity Administrator.

Messages that are addressed to an imported list are sent to all members of the list—including those who are not Cisco Unity subscribers—unless you import non-universal groups from Exchange. When you import non-universal groups, all of the public distribution list members may not receive messages as expected. For more information on this Exchange limitation, see the Microsoft website.

Use the following procedures to create or modify a public distribution list, and to add or remove subscribers from a list.

To Create a Public Distribution List

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Public Distribution List dialog box, enter information as applicable in the Name field.

Step 4 Do one of the following:

- Select **New Distribution List**.
- Select **Based on Existing Distribution List**, and then select the applicable distribution list in the Based On field.

- Select **Import**, and then click **Select**. In the Find and Select Public Distribution List to Import dialog box, click the applicable domain from the Domain list, complete the Find By fields, and click **Find**. Double-click the applicable public distribution list.

Step 5 Click the **Add** button.

Step 6 Enter settings for your new distribution list, and then click the **Save** icon.

To Modify a Public Distribution List

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.

Step 2 Click the **Find** icon.

Step 3 On the Find and View Distribution List dialog box, in the Find By field, select Name or Dial ID search criteria, then enter the name or Dial ID of a distribution list to modify. You also can enter ***** for a list of all distribution lists, or enter one or more characters of the name or Dial ID followed by ***** to narrow your search.

Note Only one asterisk can be used when doing a wild card search, and the asterisk must be the last character in the search string. For example, the search string co* is allowed; the search strings *co and *co* are not allowed.

Step 4 Click **Find**.

Step 5 Double-click the distribution list that you want to modify.

Step 6 Change settings as applicable, and then click the **Save** icon.

To Add or Remove Subscribers from a Public Distribution List

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Public Distribution Lists** page.

Step 2 Click the **Find** icon.

Step 3 Double-click the name of the list that you want to modify.

Step 4 Go to the **Subscribers > Public Distribution Lists > Members** page.

Step 5 Click **Add** or **Remove**, as applicable. If you click **Add**, select either **Selected Subscribers** or **Public Distribution Lists** from the list on the right.

Step 6 Enter the name of a subscriber or distribution list to add or remove. You also can enter ***** for a list of all subscribers or lists, or enter one or more characters followed by ***** to narrow your search.

Note Only one asterisk can be used when doing a wild card search, and the asterisk must be the last character in the search string. For example, the search string co* is allowed; the search strings *co and *co* are not allowed.

Step 7 Click **Find**.

Step 8 Select the subscriber or distribution list name to add or remove. To select more than one name, hold down the Ctrl or Shift key.

Step 9 Click **Add to List** or **Remove**, as applicable.

Specifying Subscriber Private List Settings

Private distribution lists, like public distribution lists, are used to send voice messages to more than one subscriber at a time. You can set up private lists for a subscriber in the Cisco Unity Administrator, though the subscriber is the only person who can send voice messages to the list.

Subscribers can manage their private lists by using the Cisco Unity Assistant or the phone.

On the Subscribers > Class of Service > Features page, you specify the maximum number of lists available to subscribers and the maximum number of members that subscribers can add to each list when they use the Cisco Unity conversation or the Cisco Unity Assistant to manage their lists. (There is no limit imposed on the number of members that can be added to a private list when you use Subscribers > Subscribers > Private Lists page to add members to a list.)

Note that unlike the personal distribution lists in Exchange, which are stored in Outlook on the client, private distribution lists in Cisco Unity are stored on the server with the other subscriber settings. Therefore, subscribers can address messages to private lists only over the phone or by using the Cisco Unity Inbox, not from ViewMail.

Note In the transition from a traditional voice messaging system to Cisco Unity, your organization may choose to migrate users to Cisco Unity in phases. During the migration phase, you may want to consider preventing subscribers from adding subscribers to their private lists in the Cisco Unity Assistant, and asking them not to use the Cisco Unity phone menus to do so—at least until the migration process is complete. To learn more, see the "Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant" section on page 28-8.

Specifying Subscriber Public Distribution List Settings

Subscriber Template public distribution list settings allow you to specify which public distribution lists subscribers will be assigned to. For example, you might create different templates for different work groups, and create a public distribution list for each work group.

Cisco Unity automatically creates a public distribution list called All Subscribers. You may want to associate the All Subscribers list with every subscriber template.

Create the public distribution lists before setting up subscriber templates if you plan to associate public distribution lists with templates. After the subscriber accounts are created, you can add or remove subscribers from the lists on the Public Distribution Lists > Profile Page.

CHAPTER 26

Setting Up the Cisco Unity Greetings Administrator

See the following sections in this chapter:

Cisco Unity Greetings Administrator Overview

The Cisco Unity Greetings Administrator allows you—or the call handler owner(s) that you assign—to manage call handler greetings from any phone. For example, when the office is unexpectedly closed because of bad weather, you can call Cisco Unity from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.

The owner of the call handler can be any subscriber or public distribution list. When a public distribution list owns a call handler, the Cisco Unity Greetings Administrator allows each member of the public distribution list to manage call handler greetings by using the Cisco Unity phone conversation. (Note that a call handler owner is not necessarily the message recipient.)

By using the Cisco Unity Greeting Administrator, you can do the following tasks without having to access the Cisco Unity Administrator:

- Rerecord a call handler greeting.
- Enable or disable the alternate greeting for a call handler.
- Determine which greeting is currently active for a call handler.

Setting Up the Cisco Unity Greetings Administrator

To set up the Cisco Unity Greetings Administrator, do the following tasks:

1. Set up a phone number so that you or another subscriber can call the Cisco Unity Greetings Administrator (for instructions, see the documentation for the phone system). Then add a routing rule to forward calls from the phone number that you set up to the Cisco Unity Greetings Administrator. Do the "To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator" procedure on page 26-2.

2. Assign a unique extension to the call handler. Do the "To Assign a Unique Extension to the Call Handler" procedure on page 26-2. Repeat this procedure for each call handler that you want to access by using the Cisco Unity Greetings Administrator.
3. As needed, tell call handler owners how to use the Cisco Unity Greetings Administrator. See the "Using the Cisco Unity Greetings Administrator to Manage Call Handler Greetings" section on page 26-3.

Alternatively, you can use the Custom Key Map utility to add the Cisco Unity Greetings Administrator to the options offered to subscribers at the main menu. Then, configure subscribers to use the Custom Keypad Mapping conversation. See the "Using the Custom Keypad Mapping Utility to Customize the Conversation" section on page 14-15.

Note The RSA SecurID system is not available for subscribers who use the Cisco Unity Greetings Administrator. For information on RSA SecurID, see the "Authentication for Cisco Unity Applications" 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.

To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator

Step 1 In the Cisco Unity Administrator, go to the **Call Management > Call Routing > Forwarded Calls** page.

Step 2 Click the **Add** icon.

Step 3 In the Add a Call Routing Rule – Direct dialog box, enter a name for the new routing rule, and click **Add**.

Step 4 In the Status field, confirm that **Enabled** is selected.

Step 5 In the Dialed Number field, enter the phone number that is set up for the system administrator to dial for changing call handler greetings by phone.

Step 6 In the Send Call To field, click **Greetings Administrator**.

Step 7 Change other fields for the routing rule as needed.

Step 8 In the routing table at the bottom of the page, confirm that the new routing rule is in an appropriate position with the other routing rules.

Step 9 To change the order of the routing rules, click Change Rule Order. (For information on routing rule order, see the "How Call Routing Rules Work" section on page 3-3.)

Step 10 Click the **Save** icon.

To Assign a Unique Extension to the Call Handler

Step 1 In the Cisco Unity Administrator, go to the **Call Management > Call Handlers > Profile** page.

Step 2 Click the **Find** icon, and in the Select and View dialog box, click **Find**. A list of call handlers appears.

Step 3 Click the call handler that you want to access by using the Cisco Unity Greetings Administrator and click **View**.

Step 4 In the Extension field, enter the unique extension you want to assign to the call handler.

Step 5 Click the **Save** icon.

Using the Cisco Unity Greetings Administrator to Manage Call Handler Greetings

The Cisco Unity Greetings Administrator allows you—or the call handler owner(s) that you assign—to manage call handler greetings from any phone. The owner of the call handler can be any subscriber or public distribution list.

By using the Cisco Unity Greeting Administrator, you can do the following tasks without having to access a Media Master control bar in the Cisco Unity Administrator:

- Rerecord a call handler greeting.
- Enable or disable the alternate greeting for a call handler.
- Determine which greeting is currently active for a call handler.

For example, if your office is unexpectedly closed because of bad weather, you can call Cisco Unity from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.

When you have set up the Cisco Unity Greeting Administrator for a call handler, the owner of the call handler can toggle between the alternate and standard call handler greetings, or record the call handler greeting over the phone. When a public distribution list owns a call handler, the Cisco Unity Greetings Administrator allows each member of the public distribution list to manage call handler greetings by using the Cisco Unity phone conversation.

To access the Cisco Unity Greetings Administrator, the owner of the call handler will require the following information:

- The phone number to dial for access to the Cisco Unity Greetings Administrator
- The ID of the call handler owner
- The password of the call handler owner
- The extension of the call handler

To prevent unauthorized access to Cisco Unity, make sure that the call handler owner understands that the above information should be kept confidential.

To Use the Cisco Unity Greetings Administrator to Manage Call Handler Greetings

Step 1 On the phone, dial the phone number for access to the Cisco Unity Greetings Administrator.

Step 2 At the prompt, enter the ID of the call handler owner, and press **#**.

Step 3 At the prompt, enter the password of the call handler owner, and press **#**.

Step 4 At the prompt, enter the extension of the call handler.

Step 5 Follow the Cisco Unity conversation to toggle between the alternate and standard call handler greetings, or to record the call handler greeting.

Toggle between greetings	Press **1**.
Record the greeting	Press **2**.

CHAPTER 27

Recording Greetings and Names

See the following sections in this chapter:

Recordings Overview

You can record names for subscribers, public distribution lists, private lists, and call handlers (including interview handlers and directory handlers), and greetings for subscribers and call handlers, by using a Media Master control bar on the pages within the Cisco Unity Administrator. In addition, in circumstances when you cannot access the Cisco Unity Administrator, you can access the Cisco Unity Greetings Administrator from any phone to manage greetings for call handlers.

Before you begin recording subscriber and call handler names and greetings, consider the following:

- Who will record the greetings? For example, do you want to hire a professional to record the call handler greetings?
- What will the greetings say? Write detailed scripts for the greetings before beginning to record.

Note that subscribers can record their own names and personal greetings by accessing the Cisco Unity conversation by phone, or by using a Media Master on the pages within the Cisco Unity Assistant. For more information on setting up subscribers to record names and greetings, see the "Setting Up the Media Master" section on page 28-10.

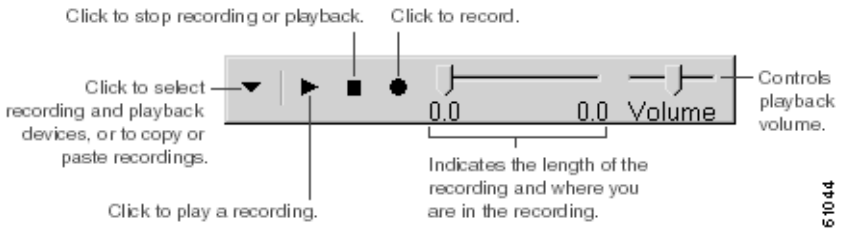
For information about using the Cisco Unity Greetings Administrator, see the "Setting Up the Cisco Unity Greetings Administrator" chapter.

Using the Media Master to Record Greetings and Names

The Media Master control bar appears on each page of the Cisco Unity Administrator on which recordings can be made. See Figure 27-1. It allows you to make and play recordings, either with a phone or with your computer microphone and speakers, by clicking the Media Master controls.

The Media Master control bar relies on DCOM (Distributed Component Object Model), and does not work through a firewall that blocks DCOM communications. It also requires that your browser is able to download and run ActiveX controls.

Figure 27-1 Media Master Control Bar



See Table 27-1 for an overview of the Media Master Options menu.

Table 27-1 Media Master Control Bar Options Menu

Option	Meaning
New	Use this option to start a new recording.
Paste	Paste a copied recording of a voice message, name, or greeting into this recording.
Paste from file	Paste a WAV file that you have stored on your computer into this recording. Note that when you do, the file is converted (if applicable) and saved on the Cisco Unity server in the G711 format—even when this is not the recording and storage codec specified for the Cisco Unity server. (For consistent sound quality, the codec format of all greetings and recorded names should match the message recording and storage codec being used by Cisco Unity. You can view the codec format of greetings and recorded names by using the Codec Checker utility. You change the codec format for greetings and recorded names by using the Set WAV Format utility. Both utilities are available in the Cisco Unity Tools Depot.)
Copy	Copy this recording so that you can paste it into another voice message, name, or greeting recording.
Copy to file	Save this recording as a WAV file to a location that you specify.
Playback devices	Select the phone or the multimedia speakers used with your computer. If you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name.
Recording devices	Select the phone or the multimedia microphone used with your computer. Note that if you select the phone, you must click Options on the Media Master Control Bar Options menu and enter an extension and server name.
Options	Enter an extension and the Cisco Unity server name here when you want to use the phone as the playback and recording device for the Media Master.

Determining Which Recording and Playback Device to Use

When determining the recording and playback device that you want to use with the Media Master in the Cisco Unity Administrator, consider the following points:

- The phone serves as the default recording and playback device for the Media Master.
- The phone offers the best sound quality for recordings.

  In order to use the phone as a recording and playback device, Cisco Unity must have at least one port assigned for a TRAP Connection per session on the System > Ports page. (See the "Voice Messaging Port Settings" section on page 11-2 for more information.) Alternatively, when you make and play recordings by using a computer microphone and speakers, no ports are used, which decreases the load on the Cisco Unity server and leaves ports open for other functions.

For a "behind the scenes" summary of how the Media Master works with a given recording and playback device, see the "What Happens When Subscribers Use the Phone as Their Recording and Playback Device" section on page 28-12 and the "What Happens When Subscribers Use a Computer Microphone and Speakers as Their Recording and Playback Device" section on page 28-13.

- When you use the phone as a recording device, the recording and storage codec specified for the Cisco Unity server determines the format in which the recordings are saved and stored on the Cisco Unity server. However, when you use a computer microphone as the recording device, your recordings are saved and stored in the G711 format—even when this is not the recording and storage codec specified for the Cisco Unity server.

  (For consistent sound quality, the codec format of all greetings and recorded names should match the message recording and storage codec being used by Cisco Unity. You can view the codec format of greetings and recorded names by using the Codec Checker utility. You change the codec format of greetings and recorded names by using the Set WAV Format utility. Both utilities are available in the Cisco Unity Tools Depot.)

Selecting a Recording and Playback Device

Use the following procedure to change the recording and playback device used by the Media Master. Updates to the Media Master are saved per user, per computer. If you plan to use another computer to access the Cisco Unity Administrator, the Media Master needs to be updated on the second computer as well.

To Select a Recording and Playback Device

Step 1 Go to any **Media Master** control bar in the Cisco Unity Administrator.

Step 2 From the Options menu, click **Playback Devices**. (The Options menu button is on the far left of the Media Master control bar. See Figure 27-1.)

Step 3 Select the device that you want to use from the list.

The <Use Preferred Device> option refers to the recording and playback devices that you have already selected for your computer (click **Settings > Control Panel > Sounds and Multimedia** on the Windows Start menu to set your preferred devices). See the Windows Help for more information on preferred recording and playback devices.

Step 4 From the Options menu, click **Recording Devices**, and repeat Step 3.

CHAPTER 28

Setting Up Subscriber Workstations

Cisco Unity subscribers can send and manage voice, fax, and e-mail messages by using a touchtone phone, or by using Cisco Unity ViewMail for Microsoft Outlook. They can also send and manage voice and fax messages by using the Cisco Unity Inbox. In addition, subscribers can use the Cisco Unity Assistant to personalize the Cisco Unity phone settings that control how they interact with Cisco Unity by phone.

This chapter reviews the preparations necessary for setting up and customizing Cisco Unity applications so that subscribers can access and use them at their workstations. See the following sections for details:

- Task List for Setting Up Subscriber Phones and Customizing the Conversation, page 28-2—Lists the tasks that you must do before subscribers access Cisco Unity by phone.
- Securing and Changing Cisco Unity Phone Passwords, page 28-3—Summarizes how Cisco Unity phone passwords are assigned, secured, and changed.
- Setting Up Cisco Unity ViewMail for Microsoft Outlook, page 28-3—Lists the tasks for setting up e-mail clients for Unified Messaging subscribers.
- Setting Up the Cisco Personal Communications Assistant, page 28-5—Summarizes what you must do so that subscribers can use the Cisco Personal Communications Assistant to access the Cisco Unity Assistant and the Cisco Unity Inbox.
- Securing and Changing Cisco PCA Passwords, page 28-9—Describes how subscriber passwords are changed and secured.
- Defining Cisco PCA Logon, Password, and Lockout Policies, page 28-10—Summarizes the account policy options that are available for Cisco PCA logons, passwords, and lockouts.
- Setting Up the Media Master, page 28-10—Explains how subscribers use the Media Master to make and play recordings over the phone, or by using the computer microphone and speakers, and what you need to do to allow them to use the preferred devices.
- Setting Up FaxMail, page 28-13—Summarizes what you must do so that subscribers can use FaxMail.
- Setting Up Mobile Message Access for BlackBerry, page 28-14—Summarizes what you must do to allow subscribers to access Cisco Unity voice messages by using their Blackberry devices.
- If you plan to set up text message notifications for subscribers (in addition to the message waiting indicators (MWIs) that you set up), also see the "Setting Up Text Message Notifications" section on page 23-2.

When you have set up subscribers to use the Cisco Unity client applications, review the tasks in the "Subscriber Orientation" chapter to orient subscribers and operators to Cisco Unity.

For a list of supported versions of Cisco Unity combined with the supported versions of the software on subscriber workstations, see the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.

Task List for Setting Up Subscriber Phones and Customizing the Conversation

As applicable, do the following tasks before subscribers access Cisco Unity by phone.

1. Set up Cisco Unity to handle busy and unanswered calls—Enable call forwarding to Cisco Unity for each subscriber phone, so that busy and unanswered calls to the subscriber extension are transferred to Cisco Unity to handle. Cisco Unity then uses the call transfer settings specified for each subscriber in the Cisco Unity Administrator to determine, for example, whether callers will be put on hold or sent directly to the subscriber greeting.
2. Specify a "Messages" button for subscriber phones—Enable each subscriber phone so that the subscriber can use a "Messages" button or a similar speed-dial button on the phone to dial the internal Cisco Unity phone number for your organization. This makes calling Cisco Unity to check messages or to change personal settings by phone quick and easy for the subscriber, as the subscriber does not have to dial the number for Cisco Unity from his or her desk phone.
3. Specify phone and TTS languages for prompts—Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers; TTS languages are the languages in which Cisco Unity can play e-mail messages over the phone. See the "Managing Languages" chapter for information on specifying phone and TTS languages.
4. Install TTY prompts—A TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call Cisco Unity and use the same features that a hearing caller can use.

   However, note the following exceptions:

   - TTY tones are not available for use in navigating through the Cisco Unity conversation.
   - Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.

   To install the TTY prompt set, see the "TTY Overview" section on page 10-9.
5. Change conversation defaults and enable conversation-specific features—Depending on your organization, you may want to change some default settings for the Cisco Unity conversation to ensure that subscribers have an easier transition from a previous voice messaging system. For example, you can change the default conversation style so that subscribers hear menus that offer a more familiar keypad mapping, and you can specify that Cisco Unity prompts subscribers to record first and then address when they send messages.

   In addition, you can enable features such as "Easy" Sign-In, system transfers, Text to Speech, and live reply. For a complete list of customizations and features, as well as details on how to implement them, see the "Summary of How You Can Customize Cisco Unity Conversations" section on page 14-1.

Securing and Changing Cisco Unity Phone Passwords

You can change the phone password for an individual subscriber on the Subscribers > Subscribers > Phone Password pages in the Cisco Unity Administrator at any time. Alternatively, you can use the Cisco Unity Bulk Import wizard to change the phone passwords for multiple subscribers at the same time. (See the Cisco Unity Bulk Import Help for details.)

As a best practice, each subscriber should be assigned a unique password that is eight or more digits long and non-trivial. If you allow subscribers to set their own passwords, encourage them to follow the same practice or use the settings on the Subscribers > Account Policy > Phone Password Restrictions page in the Cisco Unity Administrator to require them to do so.

When their accounts are configured to allow them, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Neither the Cisco Unity conversation nor the Cisco Unity Assistant require subscribers to enter their old phone passwords to reset them.

Note that AMIS, Bridge, Internet, and VPIM subscribers cannot log on to Cisco Unity by phone, use the Cisco Unity Assistant, or use the Cisco Unity Inbox.

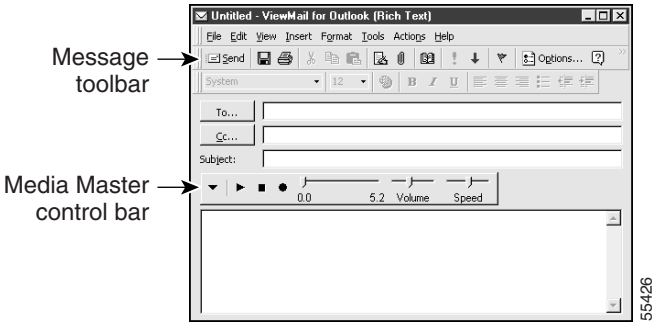
Related Documentation

- For information on specifying the minimum length for phone passwords, and the other ways in which you can secure phone access, such as specifying that Cisco Unity check for trivial passwords, prohibit the use of blank phone passwords and passwords that never expire, and maintain a record of previously used passwords, 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.
- For additional security, you can set up Cisco Unity subscriber accounts to use a secure logon method known as two-factor user authentication. To learn more, see the "Authentication for Cisco Unity Applications" 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.
- For suggestions on how to handle distributing initial phone passwords to subscribers, see the "Subscriber Orientation" section on page 29-1.

Setting Up Cisco Unity ViewMail for Microsoft Outlook

By using ViewMail, Cisco Unity subscribers can send and manage voice, fax, and e-mail messages from their Outlook Inbox. Subscribers can use ViewMail to send voice messages to other subscribers, to non-Cisco Unity subscribers, and to public distribution lists. They can play and record voice messages by using the Media Master control bar, as depicted in Figure 28-1. (Cisco Unity may require that subscribers enter their credentials when they use the phone as a playback or recording device for the Media Master, such as when subscriber workstations are in a different domain than Cisco Unity.)

Figure 28-1 Cisco Unity ViewMail for Microsoft Outlook



Task List for Setting Up Cisco Unity ViewMail for Microsoft Outlook

ViewMail is not a licensed feature, nor does it require that you give subscribers special class of service (COS) privileges or passwords to use it. However, ViewMail must be installed on each subscriber workstation. Complete the following tasks to set up ViewMail for subscribers:

1. Review the *Release Notes for Cisco Unity ViewMail for Microsoft Outlook*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. The document specifies the requirements and procedures for installing ViewMail.
2. Optional: Set up ViewMail to download messages before playing them and to save only the message headers for sent messages. See the "Customizing ViewMail for Optimal Performance" section on page 28-4.

Customizing ViewMail for Optimal Performance

If subscribers play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), they should download messages before playing them for best performance and quality. (By default, messages are streamed from the Cisco Unity server during playback.)

You can also customize ViewMail to reduce the amount of disk space needed for storing sent messages on subscriber workstations, so that it saves only the message headers for voice messages that subscribers send, and not the message recordings.

Use the following procedures to set up either of these options on subscriber workstations. Subscribers can also see ViewMail Help or the *Cisco Unity User Guide* to set up these options on their own.

To Download Messages Before Playing Them

Step 1 On the Outlook Tools menu, click **ViewMail Options**.

Step 2 Click the **Playback** tab.

Step 3 Check the **Download Audio Before Playing** check box.

Step 4 Click **OK** to save your changes.

To Save Only Message Headers

Step 1 On the Outlook Tools menu, click **ViewMail Options**.

Step 2 Click the **General** tab.

Step 3 Check the **Keep Only Message Header in the Sent Items Folder** check box.

Step 4 Click **OK** to save your changes.

Setting Up the Cisco Personal Communications Assistant

Subscribers use the Cisco Personal Communications Assistant (PCA) to access the Cisco Unity Assistant and the Cisco Unity Inbox. The Cisco Unity Assistant is a website that gives subscribers the ability to customize personal settings—including recorded greetings and message delivery options—on their workstations. The Cisco Unity Inbox website lets subscribers listen to, compose, reply to, forward, and delete voice messages, and with the fax option, manage fax messages. (The Cisco Unity Inbox is a licensed feature, and can be accessed only if it is purchased.)

The Cisco PCA is not a licensed feature, nor are subscribers required to have COS rights to access it. Any Cisco Unity subscriber can access the Cisco PCA at http://<Cisco Unity server>/ciscopca. (Note that the URL is case-sensitive.) However, subscribers do require proper COS rights to the Cisco Unity Assistant and/or the Cisco Unity Inbox.

Task List for Setting Up the Cisco Personal Communications Assistant

The Cisco PCA is installed on the Cisco Unity server during installation. To allow subscribers to access it, you do not need to install any additional files on subscriber workstations; however, you must complete the following tasks:

1. Confirm that the directory in which Cisco Unity is installed (the default directory is CommServer) and all subdirectories under that directory are excluded from virus scanning. (Typically, this is done during Cisco Unity installation.) See the virus-scanning software Help for information on excluding directories from scanning.
2. As applicable, give subscribers proper COS rights to the Cisco Unity Assistant and/or the Cisco Unity Inbox. See the "Creating, Modifying, Assigning, and Deleting Classes of Service" section on page 19-2.
3. On each subscriber workstation, configure the browser so that Cisco PCA pages display properly and the pages are presented in the appropriate language. See the "Configuring Subscriber Browsers to Use the Cisco PCA" section on page 28-6.
4. Optional: Customize the Cisco Unity Inbox to download messages before playing them. See the "Customizing Cisco Unity Inbox for Low Bandwidth Deployments" section on page 28-7.
5. Optional: Exclude return receipts from the Cisco Unity Inbox. (Return receipts are delivery and read receipts.) For details on setting up this functionality, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Exclude Return Receipts from the Inbox). The Advanced Settings tool is available in Tools Depot.

6. Optional: Specify that the Cisco Unity Inbox never asks subscribers to confirm deletions, or that subscribers are only asked to confirm their choice if deleting an item will delete it permanently. For details on setting up this functionality, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Confirm Deletes). The Advanced Settings tool is available in Tools Depot.
7. Optional: As applicable, consider changing the default search scope for the Cisco PCA Address Book so that subscribers do not need to keep track of which Cisco Unity subscribers in your organization are listed in the local directory and which are listed in the global directory. See the "Changing the Default Search Scope for the Cisco PCA Address Book" section on page 28-8.
8. Optional: If your organization is migrating from a legacy voice messaging system to Cisco Unity in phases, you may want to consider preventing subscribers from using the Cisco Unity Assistant to add individual subscribers to private lists in the interim. See the "Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant" section on page 28-8.
9. Optional: As a security precaution, you may want to prevent subscribers from saving any voice message—regardless of its sensitivity—to their hard disks by disabling the Copy to File option on the Options menu of the Media Master control bar in the Cisco Unity Inbox. To learn more, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Disable Copy to File Option in Media Master). The Advanced Settings tool is available in Tools Depot.

Configuring Subscriber Browsers to Use the Cisco PCA

To allow subscribers to access the Cisco PCA, configure their browsers to:

- Enable Active scripting
- Download and run ActiveX controls
- Enable Java scripting
- Accept all cookies
- Automatically check for newer versions of temporary Internet files
- Enable Medium-High privacy

In addition, on workstations that are running Windows Vista and Internet Explorer 7:

- For Trusted Sites, uncheck the **Enable Protected Mode** check box.
- Add the URL for the Cisco PCA website (http://<Cisco Unity server name>/ciscopca) to the list of trusted sites.

To change the GUI language used in the Cisco Personal Communications Assistant (PCA), select a language in the browser. The language selected in the browser must be one of the languages that the Cisco PCA offers. For a list of supported languages, see the "Available Languages for Cisco Unity Components" section of the applicable *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Bookmarking Web Pages

When subscriber browser settings are set to cache temporary Internet pages automatically, subscribers can create a bookmark or Favorite to access a Cisco Unity Assistant or Cisco Unity Inbox web page, but the page will be read-only. Explain to subscribers that they should bookmark the Cisco PCA home page, rather than individual pages in the Cisco Unity Assistant and the Cisco Unity Inbox. (Subscribers should not change their browser settings as a workaround; when the browser is not set to automatically check for newer versions of temporary Internet files, the Media Master control is not displayed correctly.)

Customizing Cisco Unity Inbox for Low Bandwidth Deployments

If subscribers play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), they should download messages before playing them for best performance and quality.

To customize the Cisco Unity Inbox so that messages are downloaded rather than streamed from the Cisco Unity server during playback, use the following procedure to change the registry setting on each subscriber workstation (as applicable). As a best practice, we do not recommend that you allow subscribers to set this up on their own.

To Customize the Cisco Unity Inbox to Download Messages Before Playing Them

Step 1 On the subscriber workstation, on the Windows Start Menu, click **Run**.

Step 2 Start **Regedit**.

Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the "Restoring" topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 3 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 4 Expand the registry key

HKEY_CURRENT_USER\Software\Cisco Systems\Cisco Unity\Media Master\Profiles

Step 5 For the applicable subscriber profile, expand the **Audio Playback Devices\Phone** key.

Step 6 If the DWORD value called Buffer Count does not exist, create it:

a. On the Edit menu, click **New DWORD Value**, name it **Buffer Count**, and then press **Enter**.

b. In the Edit DWORD Value window, name the new DWORD **Buffer Count** and click **Decimal**.

Step 7 Double-click the DWORD, **Buffer Count**.

Step 8 In the Value Data field, enter **3**.

Step 9 Click **OK**.

Step 10 If the DWORD value called Buffer Size does not exist, create it:

a. On the Edit menu, click **New DWORD Value**, name it **Buffer Size**, and then press **Enter**.

b. In the Edit DWORD Value window, name the new DWORD **Buffer Size** and click **Decimal**.

Step 11 Double-click the DWORD, **Buffer Size**.

Step 12 In the Value Data field, enter **300000**.

Step 13 Click **OK**.

Step 14 Close the **Registry Editor**.

You do not need to restart the workstation for the changes to take effect. TRUE?

Changing the Default Search Scope for the Cisco PCA Address Book

By default, the search scope for the Cisco PCA Address Book is set to the local directory. As a possible convenience to subscribers in your organization, you may want to change the default search scope to the global directory instead. When this is done, subscribers can search for subscribers at different locations without having to change the search scope themselves. In addition, subscribers will not need to keep track of which Cisco Unity subscribers are listed in the local directory and which are listed in the global directory.

Changing the default search scope for the Cisco PCA Address Book changes the default search scope for the following user interfaces:

- The Find Names and Check Names dialog boxes in the Cisco Unity Inbox, which subscribers use to resolve addressing when they send messages.
- The Find Names dialog box in the Cisco Unity Assistant, which subscribers use to add members to private lists.

Use the following procedure to set the global directory as the default search scope for the Cisco PCA Address Book. The change affects all subscribers that are associated with the Cisco Unity server.

Regardless of the default search scope that you specify here, subscribers can still switch between the local and global directory as they use the Cisco PCA Address Book in the Cisco Unity Inbox and Cisco Unity Assistant.

To Set the Default Search Scope to the Global Directory for the Cisco PCA Address Book

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Unity Inbox and Assistant—Set Default Address Book Search Scope**.

Step 4 In the New Value list, click **1**, and then click **Set** so that the Address Book searches for subscribers within the dialing domain.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

You do not need to restart Cisco Unity to enable the change.

Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

In the transition from a legacy voice messaging system to Cisco Unity, your organization may choose to migrate users to Cisco Unity in phases. As a result, Cisco Unity will likely support both regular subscribers and "external" subscribers—Bridge, AMIS, or VPIM contacts (as applicable)—at the same time. Regular subscribers can send messages to external subscribers, and even add them to their private distribution lists during the transition.

However, once external subscribers are converted into regular Cisco Unity subscribers, they are automatically removed from all private lists without notifying private list owners. When this occurs, subscribers may continue to send messages to their private lists without realizing that some of their intended recipients no longer receive them.

When convenient and practical, Cisco Unity Administrators should notify subscribers when external subscribers are converted to regular subscribers, notifying subscribers that they should re-add the newly migrated subscribers to existing private lists, as applicable. During the migration phase, you may also want to consider preventing subscribers from adding subscribers to their private lists in the Cisco Unity Assistant, and asking them not to use the Cisco Unity phone menus to do so—at least until the migration process is complete.

Use the following procedure to prevent all subscribers who are associated with the Cisco Unity server from adding individual subscribers to their private lists in the Cisco Unity Assistant. The procedure does not prevent subscribers from using the Cisco Unity phone menus to add regular and external subscribers to their private lists, nor does it prevent subscribers from addressing messages to regular and external subscribers.

To Prevent Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Unity Assistant—Do Not Allow Subscribers to Add Subscribers to Private Lists**.

Step 4 In the New Value list, click **1**, and then click **Set** so that when subscribers add members to their lists in the Cisco Unity Assistant, the Find Names dialog box does not display the Subscribers tab. (Subscribers can continue to add distribution lists to their lists from the Distribution Lists tab.)

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

You do not need to restart Cisco Unity to enable the change.

Securing and Changing Cisco PCA Passwords

Subscribers enter their Active Directory account user names and passwords to log on to the Cisco PCA. (Note that Cisco PCA passwords are not related to Cisco Unity phone passwords, nor are they synchronized with them.)

You can change subscriber passwords by using Active Directory Users and Computers after you create subscriber accounts. Each subscriber should be assigned a unique password. It is a good idea to specify a long—eight or more characters—and non-trivial password. Encourage subscribers to follow the same practice whenever they change their passwords, or set your domain account policy in Active Directory to require them to do so. Subscribers cannot use the Cisco Unity phone conversation or the Cisco Unity Assistant to change their Cisco PCA passwords, nor can administrators change them in the Cisco Unity Administrator. Instead, subscribers can change their Cisco PCA passwords only in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is in a different domain than the one that subscribers typically access with their Active Directory passwords, subscribers will need to specify the domain name for the Cisco Unity server.)

Note Subscribers may assume that their phone and Cisco PCA passwords are the same. As a result, they may think that they are changing both passwords when Cisco Unity prompts them to change their phone password during first-time enrollment. For this reason, you may find that many subscribers do not consider securing their Cisco PCA passwords in Windows, even though you request that they do so.

The initial password that subscribers use to access the Cisco PCA depends on how the subscriber accounts were created.

Related Documentation

To understand how authentication works with the Cisco PCA, and any security issues that may affect your organization, see the "Authentication for Cisco Unity Applications" 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.

Defining Cisco PCA Logon, Password, and Lockout Policies

The account policy that you specify on the Authentication page in the Cisco Unity Administrator determines how Cisco Unity handles situations when subscribers attempt to log on to the Cisco PCA and repeatedly enter incorrect passwords; whether subscribers can use blank passwords; the number of failed logon attempts that Cisco Unity allows before the subscriber account cannot be used to access the Cisco PCA; and the length of time that a user remains locked out.

In addition, you can use the settings on the Authentication page to specify whether the Log On page for the Cisco PCA offers subscribers the following options:

- Remember User Name
- Remember Password
- Remember Domain

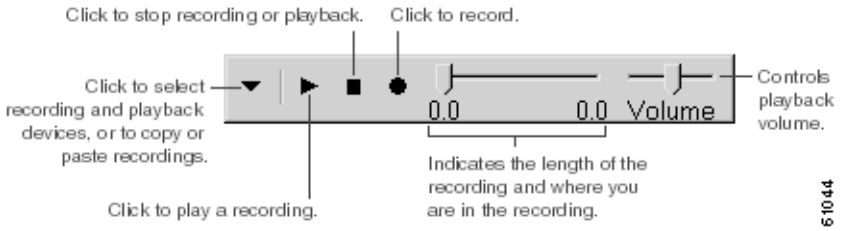
When subscribers specify that Cisco Unity will remember their user name, password, or domain, subscribers will not have to enter them the next time that they log on to the Cisco PCA. Instead, the fields are automatically populated in the Log On page. Allowing subscribers to specify whether Cisco Unity will remember their credentials may reduce support desk requests for the information. However, you may not want the Log On page to offer subscribers the above options for security reasons. If this is the case, you can uncheck the Remember Logons for __ Days check box on the Authentication page to prevent the options from appearing on the Cisco PCA Log On page, and to require that subscribers enter their user name, password, and domain each time that they log on to the Cisco PCA.

To customize the logon, password, and lockout policies that Cisco Unity applies when subscribers use the Cisco PCA to access Cisco Unity, see the "Authentication Settings" section on page 11-1.

Setting Up the Media Master

The Media Master control bar appears on each page of the Cisco Unity Assistant and the Cisco Unity Inbox where subscribers can make and play recordings—either by using the phone, or by using the computer microphone and speakers and clicking the Media Master controls. See Figure 28-2.

Figure 28-2 Media Master Control Bar



The first time that subscribers open a Cisco Unity Assistant or a Cisco Unity Inbox page that contains the Media Master (or when they access a web page that contains the Media Master and there is a newer version available), subscribers are prompted to install it. If they choose not to install, subscribers will be prompted to install each time that they visit a web page which contains the Media Master. When they indicate that they want to install it, the Media Master installs automatically, as long as subscribers have local administrative rights to their workstations. On subsequent visits to web pages that contain the Media Master, it is created from the locally installed copy.

To learn more about how the Media Master works and how to set up subscriber workstations to use it, see the following sections:

- Task List for Setting Up the Media Master, page 28-11
- What Happens When Subscribers Use the Phone as Their Recording and Playback Device, page 28-12
- What Happens When Subscribers Use a Computer Microphone and Speakers as Their Recording and Playback Device, page 28-13
- How Subscribers Specify Their Recording and Playback Device Preferences, page 28-13

Task List for Setting Up the Media Master

Compete the following tasks before subscribers start using Cisco Unity applications that offer the Media Master:

Note The Media Master control bar relies on DCOM (Distributed Component Object Model), and does not work through a firewall that blocks DCOM communications. Keep this in mind when setting up subscribers for remote access.

1. To allow subscribers to use the phone as a recording and playback device, specify that Cisco Unity has at least one voice messaging port designated for this purpose (see the "Voice Messaging Port Settings" section on page 11-2 for more information). Alternatively, provide sound cards, speakers, and microphones to subscribers who do not want to use the phone as their recording and playback device.

   When determining which recording and playback devices that you want subscribers to use, the same considerations apply as when you select the device to use with Media Master in the Cisco Unity Administrator. Review the "Determining Which Recording and Playback Device to Use" section on page 27-2 for the list of considerations.

2. Configure subscriber browsers to download and run ActiveX controls or tell subscribers to do so. Also, make sure that subscribers have local administrative rights to their workstations so that the Media Master installs properly. (Subscribers who do not have their browsers configured to download and run ActiveX controls or do not have the Media Master properly installed will see a red X instead of Figure 28-2.)
3. For subscribers who will play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), set up Cisco Unity ViewMail for Microsoft Outlook and the Cisco Unity Inbox to download messages before playing them; this will result in the best performance and quality. As applicable, see the "Customizing ViewMail for Optimal Performance" section on page 28-4 and the "Customizing Cisco Unity Inbox for Low Bandwidth Deployments" section on page 28-7.
4. For subscribers who use Cisco Unity ViewMail for Microsoft Outlook, disable personal firewalls on their workstations, or remove the applicable software. Security software that offers personal firewalls for individual workstations causes ViewMail to stop functioning when subscribers use the phone as a playback device. Alternatively, set up subscriber workstations so that they can play messages in ViewMail with computer speakers.

What Happens When Subscribers Use the Phone as Their Recording and Playback Device

When subscribers use the phone as a recording and playback device in the Cisco Unity Administrator, the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail, the following occurs:

1. The subscriber clicks the applicable option in the Cisco Unity application to make or play a voice recording.
2. When subscriber workstations are in a different domain than the Cisco Unity server, Cisco Unity will prompt subscribers to enter credentials. Subscribers are only prompted to enter their credentials once per Outlook session.
3. The Cisco Unity application asks the Cisco Unity server to place a call to the extension specified in the Media Master, and Cisco Unity calls the extension.

   By default, when Cisco Unity makes the call, it waits for the subscriber phone to ring four times before displaying the message, "The specified phone number does not answer." You can adjust the maximum number of rings that Cisco Unity waits for when making such calls. See Advanced Settings tool Help (in the Unity Settings list, click Administration—Set Maximum Number of Rings to Wait For TRAP Calls). The Advanced Settings tool is available in Tools Depot.
4. When making a recording, the subscriber answers the phone, and records the message, name, or greeting. The recording and storage codec specified for the Cisco Unity server determines the format in which the recording is saved and stored on the Cisco Unity server. When the subscriber hangs up, the Cisco Unity application tells the Cisco Unity server that the recording is finished.

   When playing a recording, the subscriber answers the phone, and the application asks Cisco Unity to play the message. Cisco Unity streams the recording over the phone.

What Happens When Subscribers Use a Computer Microphone and Speakers as Their Recording and Playback Device

When subscribers use a computer microphone and speakers as a recording and playback device in the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail, the following occurs:

1. The subscriber clicks the applicable option in the Cisco Unity application to make or play a voice recording.
2. When making a recording, the subscriber begins speaking into the microphone. When the subscriber clicks the applicable option to stop recording, the Cisco Unity application tells the Cisco Unity server that the recording is finished. The recording is saved and stored in the G711 codec format—even when this is not the recording and storage codec specified for the Cisco Unity server. The same is true when the subscriber uses the Paste option on the Media Master control bar to insert a WAV file that is stored on the computer into the recording; the file is converted (if applicable) and saved on the Cisco Unity server in the G711 format.

   When playing a recording, Cisco Unity streams the message to the client application. Streaming occurs on demand, regardless of network traffic. The client application begins to play the message through the speakers as soon as a few seconds of the message are buffered in memory on the subscriber workstation.

How Subscribers Specify Their Recording and Playback Device Preferences

Subscribers can set their own recording and playback device preferences from the Media Master Options menu. Refer subscribers to the "Overview: Changing Recording and Playback Settings" chapter of the *Cisco Unity User Guide*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

Media Master recording and playback settings are saved per user, per workstation. This means that:

- A subscriber who is logged on to the Cisco PCA or ViewMail can change recording and playback devices from any Media Master Options menu. The recording and playback devices that a subscriber chooses apply to all Cisco Unity applications, as long as the subscriber accesses the applications from the same workstation on which the changes were initially made.
- If multiple subscribers share the same workstation, each subscriber who uses the workstation must indicate a choice of recording and playback devices.
- If a subscriber has updated the choice of recording and playback devices from one workstation, but also accesses the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail on a different workstation (for example, from a computer at home), the choice of recording and playback devices must be indicated for the second workstation as well.

Setting Up FaxMail

Integrating a fax server with Cisco Unity allows to subscribers to manage their fax messages.

To allow subscribers to manage fax messages over the phone or from the Cisco Unity Inbox, assign them to a class of service (COS) that has FaxMail enabled. (All Unified Messaging subscribers, regardless of COS, can manage fax messages in their e-mail Inboxes.)

Setting Up Mobile Message Access for BlackBerry

The Mobile Message Access for BlackBerry is not a licensed feature, nor does it require that you give subscribers special class of service (COS) privileges. As long as their Blackberry devices are connected to a Blackberry server that has a Mobile Message Access for BlackBerry plug-in installed, and the devices are configured properly, subscribers can use their Blackberry devices to access Cisco Unity voice messages on a Cisco Unity server that is set up for Unified Messaging.

Voice messages appear along with other messages in the BlackBerry Inbox. To play a Cisco Unity voice message, subscribers use their BlackBerry device to open the message and click the associated link. Cisco Unity calls the phone number specified for message playback, and when the subscriber answers the call, the message begins to play. (Note that the restriction tables associated with the subscriber class of service may prohibit them from specifying certain phone numbers for message playback.)

The menu options available during and after message playback are the same as those available when subscribers log on to Cisco Unity to play messages over the phone. After saving or deleting a message, subscribers can select another message from the BlackBerry Inbox to play, or they can press * to log on to Cisco Unity to perform other tasks.

Task List for Setting Up Mobile Message Access for BlackBerry

Do the following tasks to set up Mobile Message Access for BlackBerry:

1. Optional: Set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol in its communications with the BlackBerry server so that the data exchanged between the Cisco Unity server and the BlackBerry server is sent over an encrypted HTTPS connection. In addition, consider preventing the BlackBerry device from displaying the resulting security alert.

   For detailed instructions, see the task list in the "Manually Setting Up the System to Use SSL" section in the "Using SSL to Secure Client/Server Connections" chapter of the *Security Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

2. To allow subscribers to use the phone as a recording and playback device, specify that Cisco Unity has at least one voice messaging port designated for this purpose.

   For more information, see the "Voice Messaging Port Settings" section on page 11-2.

3. Install the Mobile Message Access for BlackBerry plug-in on the BlackBerry server. See the *Release Notes for Cisco Unity Mobile Message Access for BlackBerry* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. The document specifies the requirements and procedures for installing the Mobile Message Access for BlackBerry plug-in.

4. Provide subscribers with the procedures in the *User Guide for Mobile Message Access for BlackBerry* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

   In addition, the first time that they use the BlackBerry device to access Cisco Unity voice messages, they will need to specify the phone number that Cisco Unity calls to play messages.

CHAPTER 29

Subscriber Orientation

Subscribers and operators in your organization need information about Cisco Unity that is specific to your installation. In addition, if your organization has a support desk, the staff will need to be prepared to answer the questions that subscribers may ask, and will need to be aware of the resources that are available to assist them in answering subscriber questions. This chapter reviews the preparations for orienting and training subscribers, operators, and support desk employees to Cisco Unity.

See the following sections:

Subscriber Orientation

After you create subscriber accounts and set up the client applications that subscribers will use to access Cisco Unity from their phones and computers, give subscribers the information described in this section to acquaint them with Cisco Unity. If you are planning supplemental Cisco Unity training, also consider reviewing the potential subscriber concerns and misconceptions listed in the "Support Desk Orientation" section on page 29-7.

Subscribers can refer to the Cisco Unity user guides or to Cisco Unity Assistant Help for further guidance after orientation.

Cisco Unity Phone Menus and Shortcuts Wallet Card

Use the Wallet Card wizard to produce the card. The templates in the wizard list frequently used menu options and shortcuts for managing Cisco Unity messages and personal options by phone; the wizard fills in the applicable touchtone keys based on the Custom Keypad Mapping conversation. The resulting PDF file is formatted as a wallet card that can be cut out and folded by subscribers.

Note Procedures in the *User Guide for the Cisco Unity Phone Interface* do not contain the keys that users press for Cisco Unity menu options. Instead, the procedures use the prompts that users hear to specify the menu options to choose. To provide users with key press information, you must use the Wallet Card wizard.

The wizard also allows you to customize technical support information and instructions for logging on to Cisco Unity. Keypad maps of the conversations provided with Cisco Unity (for example, the standard conversation and Alternate Keypad Mapping N) are available for printing out as well. The Wallet Card wizard is launched from the Custom Key Map utility in the Cisco Unity Tools Depot. For more information, see the "Documenting Your Key Map" section in Custom Key Map Help.

Applicable User Guides

The following Cisco Unity user guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html:

- *User Guide for the Cisco Unity Phone Interface*
- *User Guide for the Cisco Unity Assistant Web Tool*
- *User Guide for the Cisco Unity Inbox Web Tool*
- *User Guide for Accessing Cisco Unity Voice Messages in an E-Mail Client*
- *User Guide for Mobile Message Access for BlackBerry*

Information in the guides is generally organized by feature. You can distribute the applicable guides for the interfaces that subscribers are using, or you can distribute feature-specific information to subscribers for whom you have enabled the features. (On Cisco.com, click the link for the topics you want, and print the PDF files.)

URL for Cisco PCA Website

Give subscribers the URL for the Cisco PCA website: http://<Cisco Unity server name>/ciscopca. Subscribers use the Cisco PCA to access the Cisco Unity web tools—the Cisco Unity Assistant and the Cisco Unity Inbox—as applicable. Subscribers enter their Active Directory account usernames and passwords to log on to the Cisco PCA.

Cisco Unity Assistant Web Tool

Provide training for subscribers to personalize their own Cisco Unity settings by using the Cisco Unity Assistant web tool, as summarized in Table 14-1 on page 14-12. In particular, subscribers may benefit from a hands-on demonstration of the Cisco Unity Assistant, as they may not be accustomed to using a web interface to set voice messaging options. Also consider sending a system broadcast message to summarize the tasks that subscribers can do when they access Cisco Unity by phone. (See the "Using the Cisco Unity Broadcast Message Administrator and the Cisco Unity Broadcast Message Administrator Tool to Send and Manage System Broadcast Messages" section on page 24-6 for details.)

Phone Menu Differences

Depending on the menu options with which subscribers in your organization are familiar, you may want to provide them with a list of phone menu differences between Cisco Unity and a previous voice messaging system—especially if you chose not to offer them an alternative to the standard conversation, which is specified by default in {Default Subscriber} template.

Cisco Unity Phone Numbers

Give subscribers the phone numbers that they dial to access Cisco Unity from within your organization and from outside the organization. As applicable, show subscribers which button or key to use on their desk phones to access Cisco Unity.

Also give them the name and extension of the Cisco Unity system administrator and any support desk contact information. There are spaces to record phone numbers and contacts in the *Cisco Unity Phone Menus and Shortcuts* wallet card.

Phone Passwords

Provide subscribers with their initial phone passwords. Alternatively, tell subscribers to set their phone passwords in the Cisco Unity Assistant web tool before they call Cisco Unity to complete first-time enrollment. (Access to the Cisco Unity Assistant is provided through the Cisco Personal Communications Assistant website. Subscribers are not required to enter an existing phone password in order to change it in the Cisco PCA.)

When they have not done so already in the Cisco PCA, subscribers are prompted to change their phone password during first-time enrollment.

First-Time Enrollment

Make sure that subscribers know to complete first-time enrollment. Subscribers do not need to refer to any Cisco Unity documentation during enrollment. Cisco Unity indicates when the enrollment process is complete. If subscribers hang up before they have completely enrolled, none of their changes are saved and the first-time enrollment conversation plays again the next time that they log on to Cisco Unity.

The "Enrolling as a Subscriber" chapter of the *User Guide for the Cisco Unity Phone Interface* details the tasks that subscribers are asked to complete as part of enrollment.

Phone Information

Give subscribers phone-specific information, such as how to turn on live record, and discuss the potential legal issues. See the "Offering Live Record" section on page 15-10.

Password Security

Explain to subscribers how to secure their phone and Cisco PCA passwords so that they adequately protect their Cisco Unity mailboxes from unauthorized access. Detail the security guidelines for your organization. See the "Password and Account Policy Management" chapter in the *Security Guide for Cisco Unity* for best practice guidelines. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Differences in Cisco Unity Passwords

Make sure that subscribers understand that their Cisco PCA passwords are not related to their Cisco Unity phone passwords, nor are the passwords synchronized. Subscribers must use Windows to change their Cisco PCA passwords.

Feature Promotion

To help subscribers understand how Cisco Unity can help improve their productivity and to know where to find documentation, send voice messages promoting features to subscribers. You can use the sample communication scripts provided, or customize them to be specific to your organization. See the "Sample Communication Scripts" section on page 29-5 for more information.

Unified Messaging

To help subscribers make the most of Unified Messaging, make sure that they understand how it works. For subscribers who like to manage voice mail and e-mail messages separately, remind them that they can turn on the Message Type menu so that they can pick which messages to hear by type ("Press 1 for voice messages, 2 for e-mails..."). Alternatively, subscribers can use the Cisco Unity Assistant web tool to specify that Cisco Unity will play e-mail messages last when they check messages by phone. Finally, subscribers may want to create a folder in their e-mail client to store voice messages separately from other messages. Subscribers may also be able use the Copy to File option available from the Options menu on the Media Master to save voice messages as WAV files on their hard disks.

Networking Features

If you have AMIS, Internet, Bridge, or VPIM subscribers in your organization, review the *Networking Guide for Cisco Unity* and/or the *Networking Guide for Cisco Unity Bridge* for information on how Cisco Unity behaves differently for these types of subscribers, and acquaint them with the applicable details.

Also, explain to regular subscribers how to address voice messages to other locations when they use the phone, ViewMail, and the Cisco Unity Inbox web tool. As necessary for all subscribers, identify how addressing messages to other locations is different with Cisco Unity than it was with a former voice messaging system.

For detailed information, see the applicable guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Full Mailboxes

Explain how full mailboxes work with Cisco Unity. See the "Support Desk Orientation" section on page 29-7 for issues that subscribers may encounter. Refer subscribers to the *User Guide for the Cisco Unity Phone Interface* for similar information.

If your organization set up the Message Store Manager utility (available in Tools Depot) or a similar tool in Exchange to automatically purge deleted messages, make sure that you explain the deleted messages aging policy to subscribers who have class of service rights to manage their deleted messages. Otherwise, subscribers will assume that they have access to their deleted messages indefinitely.

Secure Messaging

As applicable, make sure that subscribers understand how secure messaging works and its limitations. See the "Securing Subscriber Messages" 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.

TTY

If your organization has subscribers who will use TTY and the TTY prompt set, provide training on using TTY with Cisco Unity. For more information on TTY, see the "TTY Overview" section on page 10-9.

Messages Without Specific Recipients

Make sure that subscribers who own call handlers or public distribution lists understand their responsibilities (if applicable). See the "How Cisco Unity Handles Messages Without a Specific Recipient" section on page 8-6.

Cisco Unity Greetings Administrator and System Broadcast Administrator

As applicable, tell subscribers how to use the Cisco Unity Greetings Administrator and System Broadcast Administrator. See the "Using the Cisco Unity Greetings Administrator to Manage Call Handler Greetings" section on page 26-3 and the "Using the Cisco Unity Broadcast Message Administrator and the Cisco Unity Broadcast Message Administrator Tool to Send and Manage System Broadcast Messages" section on page 24-6.

Sample Communication Scripts

To help promote new features and functionality to subscribers, Cisco Unity includes a set of sample communication scripts that describe key new features. These scripts can be customized to suit the needs of your organization, and recorded as voice messages to explain how these features can improve productivity.

Cisco Unity customers have reported some success after sending short voice messages to subscribers that describe new features and where to find more information on how to use them. This communication method may help:

- Improve the subscriber experience with Cisco Unity. These voice messages help create awareness of new features and system behaviors and advise subscribers on how they can improve their productivity.
- Facilitate the transition to Cisco Unity from a previous voice messaging system. A short message can help to reduce any surprises due to differences in system behavior, and can direct subscribers to where they learn more about how to use Cisco Unity.
- Obtain feedback from subscribers on how they use Cisco Unity and the type of information they want to receive. As part of the voice message, invite subscribers to respond to the message and provide feedback.

Task List for Using the Sample Communication Scripts

You can use the scripts as they are written, or customize them to suit the needs of your organization.

1. Review the feature scripts and determine which ones you will record as voice messages to subscribers. The scripts are text files located in the \\commserver\feature_script directory, with subdirectories for features available in specific versions of Cisco Unity.
2. Customize the scripts to suit the needs of your organization.

   Copy the script files and open them using any text editor. You can use these scripts as they are written, or edit them to be more relevant to your subscribers. You can also use these scripts as a model for writing additional messages to send to subscribers.

   When customizing the scripts, consider the following tips:

   - Keep each message short, ideally 30 seconds or less, but no more than 60 seconds, to hold the interest and attention of your subscribers. Try to focus on only one topic or feature in each message.
   - Structure each message consistently. This helps subscribers to identify these communications and to anticipate the type of information they will receive. For example, start each message the same way so that subscribers know that this is information about Cisco Unity. End each message the same way—ideally, by telling subscribers where they can get additional information about the feature.
   - Provide a place where subscribers can find more information that is easy for them to remember. For example, you could set up a web site URL, using the format http:\\www.voicemail.companyname.com, to direct users to more information on Cisco Unity. On this website, provide information and tips on the new Cisco Unity features, point to the online documentation, and create and promote educational resources for using Cisco Unity effectively and efficiently.
   - Ask for feedback. In one or all of the messages, ask subscribers to reply to the message and provide feedback. For example:

"We hope you found these voice messaging tips valuable. If you'd like to provide feedback, good or bad, about your experiences using Cisco Unity Five dot Zero, reply to this message. Your input helps us make Cisco Unity a successful tool for all employees. Thank you for your support."

This is a good way to find out what subscribers think about this method of communication and the new Cisco Unity features.

3. Determine a schedule and have a well-known employee record the voice messages.

   We recommend that you have organizational leaders or other recognizable voices record the messages. This helps to attract attention and can make the message content more meaningful and relevant to subscribers.

   In the first week after the new version of Cisco Unity is available to subscribers, set up a schedule to deliver voice messages highlighting the top new features. To avoid overwhelming your subscribers, plan to send a message every other day.

   As subscribers become more familiar with Cisco Unity, and if you have positive feedback on this communication method, you may want to plan to send additional messages on a monthly basis that highlight other Cisco Unity features or provide productivity tips.

Operator Orientation

Operator orientation should address the same points as subscriber orientation, but in greater detail. Operators must be familiar with how subscribers use Cisco Unity. Depending on the size of your organization, the operator may be the person subscribers are likely to ask when they have questions about Cisco Unity.

In addition to the items discussed in the "Subscriber Orientation" section on page 29-1 and the "Support Desk Orientation" section on page 29-7 (as applicable), operators also need to understand the following concepts and tasks:

Roles of the Operator and the Automated Attendant

The way your organization uses the automated attendant determines what the operator responsibilities are. The automated attendant is a call handler that is used in place of a human operator to answer and direct calls by playing greetings and responding to touchtones. The automated attendant can provide a menu of options (for example, "For Sales, press 1; for Service, press 2."), and it can also provide information (for example, "Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.").

Directing Calls

Regardless of how your organization uses the automated attendant, many calls will go to the operator. The operator must know how to direct calls to voice mail and to subscriber phones. To direct calls to voice mail, the operator can dial Cisco Unity and at the Opening Greeting, dial the subscriber extension and then press #2. The subscriber phone does not ring, and the transferred caller hears the subscriber greeting.

You can also create a call handler for each subscriber to send calls directly to their greetings. For details on setting this up, see the techtip, "How to Transfer a Caller Directly into a Mailbox," available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html.

Forwarding Unaddressed Messages to Intended Recipients

If an operator also owns a call handler or public distribution list, make sure that the operator knows to review unaddressed messages frequently, and to forward them to the intended recipient(s). See the "How Cisco Unity Handles Messages Without a Specific Recipient" section on page 8-6.

Using the Cisco Unity Greetings Administrator

An operator who is responsible for changing call handler greetings for the organization can use the Cisco Unity Greetings Administrator when is not practical to change a greeting in the Cisco Unity Administrator. For example, if the office is unexpectedly closed because of bad weather, the operator can call from home to use the Cisco Unity Greetings Administrator to enable the alternate Opening Greeting, or to rerecord a call handler greeting stating that the office is closed. For more information, see the "Using the Cisco Unity Greetings Administrator to Manage Call Handler Greetings" section on page 26-3.

Using the Cisco Unity Broadcast Message Administrator

If an operator will be responsible for sending recorded announcements to everyone in an organization (or to particular location(s) within an organization), explain how to access and use the Cisco Unity Broadcast Message Administrator to send broadcast messages. In particular, make sure that those who are able to send system broadcast messages to subscribers on multiple servers understand the meaning of each addressing option offered by the Cisco Unity Broadcast Message Administrator and understand how to address a message to reach subscribers on a particular group of servers. See the "Using the Cisco Unity Broadcast Message Administrator and the Cisco Unity Broadcast Message Administrator Tool to Send and Manage System Broadcast Messages" section on page 24-6.

Support Desk Orientation

Support desk orientation should address the same points as subscriber and operator orientation, but in greater detail. Support desk staff must be familiar with how subscribers and operators use Cisco Unity, and the common problems that subscribers may encounter when using Cisco Unity. Instead of using the Cisco Unity server, it may be helpful to set up a test server that support desk staff can use to browse to the Cisco Unity Administrator, and troubleshoot and test client applications.

Caution Do not install Outlook on the Cisco Unity server, or Cisco Unity may not notify subscribers of new messages.

To prepare for possible calls to the support desk at your organization, familiarize the support desk staff with the resources listed below, and with the potential subscriber concerns and misconceptions listed in the section that follows.

Support Desk Resources

- Subscriber documentation is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.
- The *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.
- The "Setting Up Subscriber Workstations" chapter provides information on how subscriber workstations should be set up, and describes how subscribers use Cisco Unity client applications and features.

- The "Cisco Unity Conversation Overview" chapter summarizes the ways in which Cisco Unity Administrators and subscribers can customize the conversation.
- The *Troubleshooting Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.
- For descriptions and the URLs of all Cisco Unity documentation on Cisco.com, see the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.
- Consider reviewing the FAQ that is tailored to address questions often asked by Cisco Unity Administrators. Some content may also be helpful to the support desk personnel in your organization. Click the link on the navigation bar in the Cisco Unity Administrator to display the FAQ.

Potential Subscriber Concerns and Misconceptions

Table 29-1 describes potential subscriber issues, which are typically based on misconceptions about how Cisco Unity works. Subscribers who encounter such issues are often those who are accustomed to another voice messaging system, were recently migrated from a previous version or a different configuration of Cisco Unity, have not yet completed Cisco Unity training, or are unaware of a new feature or functionality change to their existing system.

Table 29-1 Potential Subscriber Concerns and Misconceptions

Potential Issue	Description
Cisco PCA security alerts when using SSL	If your organization set up Cisco Unity to use SSL, but did not add it to the Group Policy in order to distribute the certificate to the trusted root store for all users in the domain (or did not tell subscribers how to add the certificate to the trusted root store on their own computers), subscribers may be concerned about the security alert that will be displayed each time that they access the Cisco PCA. Tell subscribers that they can ignore the warning and proceed to use the Cisco PCA without doing any harm to their computers or the network. To prevent the browser from displaying the security alert, see the "Using SSL to Secure Client/Server Connections" 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.

Table 29-1 Potential Subscriber Concerns and Misconceptions (continued)

Potential Issue	Description
Delayed messages	Subscribers may believe that their messages are delayed for the following reasons: • While listening to new messages, subscribers may skip a message and inadvertently mark it new. Later, when they check messages again, they hear the skipped message and believe that the message arrived after a delay. • Subscribers may skip more messages than they intend while listening to their messages, and later check messages again only to hear one or more of the skipped messages, and believe that the message(s) arrived after a delay. See the "Skipping messages" section. • When settings are changed for a subscriber in Exchange, the new values may not be reflected immediately in Cisco Unity. Explain to the subscriber that the settings may take a few minutes to synchronize, causing a delay in receipt of messages. • When subscribers have the Dropped Call Recovery feature enabled for calls dropped while addressing or recording messages, messages they send to other subscribers are not sent until after the recovery time period has expired if the message recording was terminated by hanging up rather than explicitly sending the message by pressing the # key.
Deleted messages	By default, when subscribers delete a new or saved message, Cisco Unity does not ask them to confirm the deletion. You may want to enable Cisco Unity to request confirmation from subscribers before proceeding with the deletion, especially if many subscribers do not belong to a class of service (COS) that allows them to retain and review their deleted messages.
Directory listing: Subscribers are not listed as expected	When subscribers do not have a recorded voice name, they are not listed in the phone directory and as a result, callers are not be able to find them when searching for them by name. By default, Cisco Unity prompts subscribers to record a voice name during first-time enrollment, but it does not prevent them from completing the enrollment process if they do not. To address this issue, consider the following options: • You can change whether recording a voice name is required to complete first-time enrollment. See Advanced Settings tool Help (in the Unity Settings list, click Conversation—First-Time Enrollment: Require Subscribers to Record Names). The Advanced Settings tool is available in Tools Depot. • You can provide voice names for subscribers on individual Subscriber > Profile pages in the Cisco Unity Administrator. • Subscribers with class of service rights can record their own names by using the Cisco Unity conversation or the Cisco Unity Assistant.
Fax: Attached files are not delivered to fax machines *(fax integrations only)*	Subscribers may be unaware that when they add attachments to an e-mail message and then send the message to a fax machine, Cisco Unity renders only those attachments with the file extensions specified during Cisco Unity setup. All other attachments are removed. To determine which file name extensions are currently specified or to specify new ones, see the "Third-Party Fax Integration" chapter in the *Troubleshooting Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.

Table 29-1 Potential Subscriber Concerns and Misconceptions (continued)

Potential Issue	Description
Incorrectly delivered messages	When subscribers switch from Standard Send menus to Streamline Send menus, they may continue to use old shortcuts to set special delivery options before sending a message. For example, out of habit, subscribers may press 131# to mark a message urgent and send it. In the Streamlined Send menu, using the same shortcut marks the message urgent, private, and then marks the message normal again before it is sent. As a result, the recipient receives a private message, and not the urgent message as the sender intended. As with any conversation change, make sure that subscribers understand the implications of changing from Standard to Streamlined Send menus so that they can adjust their behavior accordingly.
Mailbox fills up quickly	Subscribers may complain that their mailboxes are filling up too quickly, for any the following reasons: • Cisco Unity does not automatically delete messages when they reach a certain age. This means that subscriber messages are saved until the subscriber deletes them permanently. • When Cisco Unity is set up to provide Unified Messaging, the messages in the Sent and Deleted Items folders in Microsoft Outlook are included in the total mailbox size. • When Unified Messaging subscribers receive nondelivery receipts (NDRs) to messages that they send, their mailbox can quickly increase in size—especially if the original message included large attachments. If their e-mail clients are configured to save their sent messages, the original message and attachments are stored in their Sent Items folders and another copy is sent to their Inboxes along with the NDR, increasing their mailbox size accordingly. • Subscribers may receive messages that have been forwarded many times over, which increases message size. The original message plus all recorded or written introductions that were added during forwarding equal the total message size. As a result, subscribers who have relatively few messages stored in their mailboxes may still find that their mailboxes exceed the storage limits. • Subscriber mailboxes can fill up while subscribers are on vacation or on an extended leave of absence. To prevent this, specify that Cisco Unity will prevent callers from leaving messages when subscribers have their alternate greetings enabled. For information on how Cisco Unity handles full mailboxes, see the "How Cisco Unity Handles Full Mailboxes" section on page 8-4.

Table 29-1 Potential Subscriber Concerns and Misconceptions (continued)

Potential Issue	Description
Managing multiple message types in a single mailbox *(Unified Messaging configurations only)*	Subscribers who are new to Unified Messaging sometimes have a difficult time understanding how to manage multiple message types from a single Inbox. For example, when subscribers check messages by phone, they may try to "clean up" their "voice mailbox" by deleting all of their e-mail messages. They are surprised and frustrated when they later discover that the messages have also been deleted from their Outlook Inboxes. Other subscribers may request that Cisco Unity stop delivering e-mail messages to their "voice mailbox" altogether. To help subscribers make the most of Unified Messaging, make sure that they understand how it works. For subscribers who like to manage voice mail and e-mail messages separately, remind them that they can turn on the Message Type menu so that they can pick which messages to hear by type ("Press 1 for voice messages, 2 for e-mails..."). Alternatively, subscribers can use the Cisco Unity Assistant to specify that Cisco Unity will play e-mail messages last when they check messages by phone. Finally, subscribers may want to create a folder in their e-mail client to store voice messages separately from other messages. Subscribers can also use the Copy to File option available from the Options menu on the Media Master to save voice messages as WAV files on their hard drives.
Message notification: Repeat notification options	When a subscriber chooses not to have Cisco Unity restart notification each time a new message arrives, setting a long interval between repeat notification calls may lead the subscriber to believe that Cisco Unity is delaying notification. For recommended interval settings, see the "Repeat Notification Option Is Misunderstood" section in the "Message Notification" chapter of the *Troubleshooting Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.
MWIs	To gain an understanding of when MWIs turn on and off, what causes them to turn on and off, and what causes MWIs to behave differently than expected, see the "Message Waiting Indicators (MWIs)" chapter in the *Troubleshooting Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.
Passwords are not secure, or subscribers use the wrong password	Subscribers may assume that their phone and Cisco PCA passwords are the same or are synchronized. As a result, they may think that they are changing both passwords when Cisco Unity prompts them to change their phone password during first-time enrollment. Additionally, and they may try to use their phone password to log on to the Cisco PCA.

Table 29-1 Potential Subscriber Concerns and Misconceptions (continued)

Potential Issue	Description
Playing a "previous" message	While listening to messages, subscribers have the option to go back and play the previous message in the stack. However, note the following: • The previous message option is not available in the Alternate Keypad Mapping X conversation. • When a subscriber presses the applicable key to go back to the previous message, the current message is left in its current state (new, saved, or deleted). In effect, the subscriber skips the current message when going back to the previous message. You may consider clarifying the "previous" message behavior for your subscribers, to make sure they understand that the new, saved, and deleted message stacks are dynamic. For example, when a subscriber listens to messages in the new message stack, and either deletes or saves messages, those messages are no longer new, and are thus dynamically removed from the new message stack. If the subscriber then presses the applicable key to go back to the previous message in the stack, the result might be unexpected. The subscriber may expect to hear the message that was just played, but if the subscriber has changed the state of that message, it will no longer be in the stack. (Note that if the subscriber has moved all previous messages to other stacks, the conversation will announce "no previous message," and the current message will play again.)
Secure messaging: limitations	To gain an understanding of the limitations of the secure messaging feature, see the "Limitations of Secure Messaging" section in the "Securing Subscriber Messages" 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.
Skipping messages *(Standard conversion style only)*	If you upgraded from Cisco Unity version 4.0(3) or earlier, and/or you customized the Cisco Unity standard conversation so that subscribers can press a single # key during message playback instead of pressing ## to skip a message, you may find that some subscribers do not easily adopt the new key mapping. As a result, you may find that: • Subscribers continue to press ## during message playback, intending to skip a single message as they did before. Instead, they unwittingly skip two messages—the message being played and the subsequent message. As a result, subscribers may report that they are missing messages, that their messages are delayed, or that their MWIs remain lit even after they have listened to "all" of their new messages. • Subscribers continue to use the old shortcuts during message playback, and report that they do not work as expected. For example, subscribers may press #4 during message playback, and find that instead of Cisco Unity skipping the rest of the message and allowing them to reply to the message as before, now Cisco Unity skips the message and begins playing the next message more slowly than the skipped one. • Subscribers complain that they no longer have a way to fast-forward to the end of the message. (See the "Changing How Subscribers Skip Messages During Message Playback (Standard Conversation)" section on page 15-4 for a list of changes to all keys as a result of losing the ability to fast-forward to end of message.) For the above reasons, we recommend that you use the Custom Keypad Map utility to adjust how # behaves during message playback. (You assign subscribers to a Custom Keypad Mapping conversation on the Subscribers > Subscriber > Conversation page in the Cisco Unity Administrator.) For additional information on using the utility, see "Using the Custom Keypad Mapping Utility to Customize the Conversation" section on page 14-15.

Table 29-1 Potential Subscriber Concerns and Misconceptions (continued)

Potential Issue	Description
Speed for elements of the Cisco Unity conversation varies	Subscribers may report that the speed at which Cisco Unity plays menus, recorded names, greetings, and messages is inconsistent. For example, subscribers may report that when they listen to their messages, the message body is played at a different speed than the recorded names of subscribers who leave them messages, and the message header and footer (timestamp, message number, and so on). Note that the speed that you or subscribers specify for message playback does not affect the speed of Text to Speech (TTS) messages, receipts, or message headers and footers. TTS messages are always played at normal speed, while the speed at which Cisco Unity plays receipts, message headers, and message footers is determined by the prompt speed that is specified for the Cisco Unity conversation. Subscribers can adjust speed for prompts and messages by using the Cisco Unity Assistant.
Unsent messages	Depending on how Cisco Unity is set up at your organization, subscribers may be surprised at how Cisco Unity handles messages when calls are intentionally or unintentionally disconnected (for example, when a subscriber hangs up or when a cell phone loses its charge or signal) while subscribers are in the process of sending, replying to, or forwarding a message. Some subscribers may incorrectly assume that Cisco Unity offers a “draft” folder for unsent messages, which is not the case. See the “Handling Messages That Are Interrupted by Disconnected Calls” section on page 17-6 for details.

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W