Unified Messaging Guide for Cisco Unity Connection

Release 9.x
Revised October 2013

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

Unified Messaging Guide for Cisco Unity Connection Release 9.x

CONTENTS

Preface

See the following sections:

Documentation Conventions

Table 1 Conventions in the Unified Messaging Guide for Unified Messaging Guide for Cisco Unity Connection

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Select **OK**.) • Information that you enter. (Example: Enter **Administrator** in the Username box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to **https://<Cisco Unity Connection server IP address>/cuadmin**.)
- (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 in the navigation bar of Cisco Unity Connection Administration. (Example: In Cisco Unity Connection Administration, expand **Contacts > System Contacts**.)

The *Unified Messaging Guide for Cisco Unity Connection* 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 Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/roadmap/9xcucdg.html.

Documentation References to Cisco Unified Communications Manager Business Edition

In the Cisco Unity Connection 9.x documentation set, references to "Cisco Unified Communications Manager Business Edition" and "Cisco Unified CMBE" apply to both Business Edition version 9.0 and to Business Edition 5000 versions 9.x. The references do not apply to Business Edition 6000.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.

Further information regarding U.S. export regulations can be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

CHAPTER 1

Introduction to Unified Messaging in Cisco Unity Connection

In Cisco Unity Connection, we gathered several existing features and a new feature under the rubric of unified messaging. These features include:

- Synchronization of voice messages in Connection and Exchange mailboxes (also known as single inbox—this feature is new in Connection)
- Text-to-speech (TTS) access to Exchange email
- Access to Exchange calendars, which allows users to do meeting-related tasks by phone (for example, hear a list of upcoming meetings, or accept or decline meeting invitations)
- Access to Exchange contacts, which allows users to import Exchange contacts and use the contact information in personal call transfer rules and when placing outgoing calls by using voice commands
- Notification of upcoming Cisco Unified MeetingPlace meetings on the phone
- Scheduling and joining of MeetingPlace meetings
- Transcription of Connection voice messages (SpeechView)

This guide explains how to configure unified messaging features and, for single inbox, how to move Exchange mailboxes between servers and how to restore Exchange mailboxes.

For information about SpeechView, see the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

In Cisco Unity Connection, we gathered several existing features and a new feature under the rubric of unified messaging. These features include:

- Synchronization of voice messages in Connection and Office 365 mailboxes (also known as single inbox)
- Text-to-speech (TTS) access to Office 365 email
- Access to Office 365 calendars, which allows users to do meeting-related tasks by phone (for example, hear a list of upcoming meetings, or accept or decline meeting invitations)
- Access to Office 365 contacts, which allows users to import Office 365 contacts and use the contact information in personal call transfer rules and when placing outgoing calls by using voice commands

CHAPTER 2

Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging

See the following sections:

About Unified Messaging with Exchange in Cisco Unity Connection

See the following sections:

Accessing Exchange Email by Using Text to Speech

When Cisco Unity Connection is configured to allow access to Exchange email by using text to speech, users have the option to hear their emails read to them when they sign in to Cisco Unity Connection by phone.

Note Text to speech over Exchange 2013, Exchange 2007, and Exchange 2010 supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrug051.html.

Unity Connection uses the IMAP protocol to access emails in Exchange so that the messages can be played by using text to speech. By default, Exchange is not configured to allow IMAP access to messages. You must enable IMAP access on each Exchange server that contains emails that you want licensed Connection users to be able to access.

Note For information on enabling IMAP access to Exchange in Cisco Unity Connection 9.x, see the "Enabling IMAP Access to Exchange in Cisco Unity Connection 9.x" section of the "Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/partner/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Accessing Exchange Calendars and Contacts

When Cisco Unity Connection is configured to access Exchange calendars and contacts, Unity Connection users can do the following by phone:

- Hear a list of upcoming meetings (Outlook meetings only).
- Hear a list of the participants for a meeting.
- Send a message to the meeting organizer.
- Send a message to the meeting participants.
- Accept or decline meeting invitations (Outlook meetings only).

- Cancel a meeting (meeting organizers only).

Note Exchange 2007/2010 calendars and contacts support both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrug051.html.

Note Microsoft Outlook 2013 is not supported with Exchange 2003.

In addition, Unity Connection enables users to import Exchange contacts by using the Unity Connection Messaging Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Connection Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

If you configure a Unity Connection user for access to the Exchange calendar, you cannot also configure the user for access to Cisco Unified MeetingPlace.

Synchronizing Voice Messages in Unity Connection and Exchange Mailboxes (Single Inbox)

The synchronization of voice messages in Unity Connection and Exchange Mailboxes for single inbox (SIB) users supports both the IPv4 and IPv6 addresses.

Note

- Single Inbox over IPv6 is supported only for Exchange 2007, Exchange 2010, and Exchange 2013.
- When single inbox is configured, Outlook rules may or may not work for Single Inbox messages.

This section describes how synchronizing voice messages in Unity Connection and Exchange mailboxes works. See the following sections:

- How Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts Are Synchronized, page 2-11

You may experience delay (in order of hours) in synchronization of voice messages from Exchange server to Connection while the Resynchronize All Single-Inbox Messages SysAgent task is running. It is recommended to run the Resynchronize All Single-Inbox Messages SysAgent task during off hours.

Where Voice Messages are Stored When Single Inbox is Configured

All Unity Connection voice messages, including those sent from Cisco Unity Connection ViewMail for Microsoft Outlook, are first stored in Unity Connection and are immediately replicated to the Exchange mailbox for the recipient.

Note When Connection is configured for Single Inbox to Exchange, where a Blackberry Enterprise Server is also integrated with the Exchange server to send voice mail out to Blackberry devices, there will be a 10-15 min delay between the time the voice mail hits Exchange before the notification is picked up by the BES. To resolve the above issue you need to install BES version 5.0.03 MR5 or later.

How Single Inbox Works with ViewMail for Outlook

If you want users to use Outlook to send new Unity Connection voice messages, or to reply to or forward voice messages, and if you want the messages to be synchronized with Unity Connection:

- If you have not already done so, in Connection Administration, add SMTP proxy addresses for the Unity Connection users that are configured for single inbox. The SMTP proxy address for a user must match the Exchange email address that is specified in the unified messaging account in which single inbox is enabled.
- Install ViewMail for Outlook on user workstations. Without ViewMail for Outlook installed, voice messages are sent by Outlook as emails with .wav file attachments, and are treated as emails by Unity Connection.
- On each user workstation, associate an email account with a Unity Connection server.

Voice messages appear in the Outlook Inbox folder of the user, alongside other messages that are stored in Exchange; the voice messages also appear in the Unity Connection mailbox of the user.

When single inbox is configured, Unity Connection adds a Voice Outbox folder to the Outlook mailbox.

Private messages cannot be forwarded.

How Single Inbox Works without ViewMail for Outlook or with Other Email Clients

If you use another email client to access Unity Connection voice messages in Exchange, or if you do not install ViewMail for Outlook:

- The email client treats Unity Connection voice messages like emails with .wav file attachments.
- When a user replies to or forwards a Unity Connection voice message, the reply or forward also is treated like an email, even if the user attaches a .wav file. Message routing is handled by Exchange, not by Unity Connection, so the message is never sent to the Unity Connection mailbox for the recipient.
- Users cannot listen to secure voice messages.

- It may be possible to forward private voice messages. (When users use ViewMail for Outlook, ViewMail for Outlook prevents private messages from being forwarded.)

Note If a voice message is sent to the user of Exchange 2003, it is immediately synchronized between Unity Connection and Exchange. The .wav file attachment is displayed both in Unity Connection Web Inbox and Outlook of Exchange 2003. In Outlook WebMail Access of Exchange 2003, the email shows the attachment symbol but when the email is opened, the .wav file attachment is not displayed. Both in Outlook and OWA of Exchange 2007, Exchange 2010, and Exchange 2013, the .wav file attachment is displayed in the email.

Accessing Secure Voice Messages in the Exchange Mailbox

To play secure Unity Connection voice messages in the Exchange mailbox, users must use Microsoft Outlook and Cisco Unity Connection ViewMail for Microsoft Outlook. Without ViewMail for Outlook installed, users accessing secure voice messages see only text in the body of a decoy message; the text briefly explains secure messages.

How transcription of Voice Messages is synchronized between Cisco Unity Connection with Exchange Mailboxes

In Cisco Unity Connection, the system administrator enables the single inbox transcription functionality. To enable transcription of voice messages, Unity Connection users must configure the following services:

- Unified Messaging Service: To configure the Unified Messaging Service, see the "Creating a Unified Messaging Service to Access Exchange from Cisco Unity Connection" section of "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter in *Unified Messaging Guide for Cisco Unity Connection*. http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html
- SpeechView Transcription Service: To configure the Speech View Transcription Service, see the "Overview of SpeechView in Cisco Unity Connection 9.x" section of "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter in the *System Administration Guide for Cisco Unity Connection* guide. http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagpdf.pdf

Note that the following services are not supported with Unity Connection, if configured with single inbox:

  - Synchronization of Multiple Forward Message
  - Synchronization of transcription for user's with Exchange 2003

In single inbox, the transcription of Voice Messages is synchronized with Exchange in the following ways:

- When sender sends voice mail to Unity Connection user through Web Inbox or touchtone conversation user interface and the Unity Connection user views voice mail through various email clients, then the transcription of voice messages are synchronized, as shown in the Table 2-1.

Table 2-1 When Sender Sends Voice Mail Through Web Inbox or Touchtone Conversation User Interface

Scenarios	Web Inbox	Outlook WebMail Access/ Outlook without VMO	ViewMail for Outlook
Successful delivery of voice messages	The text of the transcription gets displayed in the reading pane of the email.	The text of transcription gets displayed in the reading pane of the email.	The text of the transcription gets displayed in the reading pane of the email and is also displayed in the transcription panel.
Failure or Response Time-out	The “Failure or Response Timeout” text gets displayed in the reading pane of the email.	The “Failure or Response Timeout” text gets displayed in the reading pane of the email.	The “Failure or Response Timeout” text gets displayed in the reading pane of the email and is also displayed in the transcription panel.
Transcription in Progress	The “Transcription in Progress” text gets displayed in the reading pane of the email.	The reading pane of the email will be blank. text.	The “Transcription in Progress” text gets displayed in the transcription panel.

- When sender sends voice mail to Unity Connection user through ViewMail for Outlook and the Unity Connection user views voice mail through various email clients, then the transcription of voice messages are synchronized, as shown in the Table 2-2:

Table 2-2 When Sender Sends Voice Maill Through ViewMail for Outlook

Scenarios	Web Inbox	Outlook WebMail Access/ Outlook without VMO	ViewMail for Outlook
Successful delivery of voice messages	The Text of transcription gets displayed in the reading pane of the email.	The text of the transcription is the part of transcript file “Transcription.txt”.	The text of the transcription is the part of transcript file “Transcription.txt” and is also displayed in the transcription panel.

Scenarios	Web Inbox	Outlook WebMail Access/ Outlook without VMO	ViewMail for Outlook
Failure or Response Time-out	The “Failure or Response Timeout” text gets displayed in the reading pane of the email.	The “Faliure or Response Time-out” text is the part of transcript file “Trancription.txt” attached in the voice message.	The “Faliure or Response Time-out” text is the part of transcript file “Trancription.txt” attached in the voice message and is also displayed in the transcription panel
Transcription in Progress	The “Transcription in Progress” text gets displayed in the reading pane of the email.	The attachment “Transcription_pending .txt” indicates the progress of transcription.	The attachment “Transcription_pending .txt” indicates the progress of transcription and the text “Transcription in Progress” is also displayed in transcription panel.

Note Voice messages received by Unity Connection, which are composed using ViewMail for Outlook have message body either with text or blank body.

- Synchronizing the transcription of voice messages, when the sender sends voice mail to Unity Connection through third-party email clients and the receiver views the voice mail through various clients.
  - The transcription of voice messages can be synchronized in either of the above mentioned scenarios.

When a sender sends a voice message to a SpeechView user, the received voice message is sent to the third-party external services for transcription. The transcription of the voice messages is sent back to Cisco Unity Connection. However, in case of any transcription failure, the third-party external service sends an error code to Connection. For more information on SpeechView transcription error codes, see “Managing Nauance Server Code in Cisco Unity Connection” chapter of the *System Administration Guide for Cisco Unity Connection*: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

For a Single Inbox (SIB) user with the SpeechView transcription service, when the **Hold till transcription received** option is enabled, the synchronization of a new voice message between Unity Connection and Exchange mailboxes will be done. The synchronization of new voice messages will be done only when Unity Connection receives the transcription of the voice message from the third-party external service. To enable the Hold till transcription received option; navigate to **Cisco Personal Communications Assistant> Message Assistant> Personal Options**.

If the **Hold till transcription received** option is enabled and Connection receives time-out/failure transcription response from the third-part external service, then the voicemail will synchronize between Connection and Exchange only when Connection receives failure/time-out transcription response.

Note By default the **Hold till transcription received** option will be disabled.

Transcription of Voice messages in Secure and Private Messages

Revised February 08, 2014

- **Secure Messages:** Secure messages are transcribed only if the user belongs to a class of service for which the **Allow Transcriptions of Secure Messages** option are enabled. This option, however, does not allow the synchronization of transcribed secure messages on the Exchange server integrated with the Unity Connection server.
- **Private Messages:** The transcription of private messages is not supported.

How Synchronization Works with Outlook Folders

Unity Connection synchronizes voice messages in the following Outlook folders with the Unity Connection Inbox folder for the user, so the messages are still visible in the Unity Connection Inbox folder:

- Subfolders under the Outlook Inbox folder
- Subfolders under the Outlook Deleted Items folder
- The Outlook Junk Email folder

Messages in the Outlook Deleted Items folder appear in the Unity Connection deleted items folder.

If the user moves voice messages (except secure voice messages) into Outlook folders that are not under the Inbox folder, the messages are moved to the deleted items folder in Unity Connection. The messages can still be played by using ViewMail for Outlook because a copy still exists in the Outlook folder. If the user moves the messages back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Unity Connection Inbox folder, and:

- If the message is still in the deleted items folder in Unity Connection, the message is synchronized back into the Unity Connection Inbox for that user.
- If the message is not still in the deleted items folder in Unity Connection, the message is still playable in Outlook, but it is not resynchronized into Unity Connection.

Connection synchronizes voice messages in the Sent Items folder with the Exchange Sent Items folder for the user. However, the changes to the subject line, the priority, and the status (for example, from unread to read) are replicated from Connection to Exchange only on an hourly basis.When a user sends a voice message from Unity Connection to Exchange, or vice versa, the voice message in the Unity Connection Sent Items folder is unread and the voice message in the Exchange Sent Items folder is marked as read.

By default, the synchronization of voice messages in the Exchange Sent Items folder with the Connection Sent Items folder is not enabled. To enable the feature, change the **Sent Messages: Retention Period (in Days)** option to a value greater than zero. To change the Sent Messages:Retention Period(in Days) option, navigate to **System Settings > Advanced > Messaging > Sent Messages: Retention Period (in Days)** in Cisco Unity Connection Administration.

For more information, see the “Messaging Configuration” section of the “Cisco Unity Connection 9.x Advanced Settings” chapter available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/gui_reference/guide/9xcucgrgx.html .

Note When a user sends the voice message to his or her voice mailbox, the voice message is not synchronized with the Exchange Sent Items folder. However, the voicemail remains in the Connection Sent Items folder.

Secure voice messages behave differently. When Unity Connection replicates a secure voice message to Exchange, it replicates only a decoy message that briefly explains secure messages; the only copy of the voice message remains on the Unity Connection server. When a user plays a secure message by using ViewMail for Outlook, ViewMail retrieves the message from the Unity Connection server and plays it without ever storing the message in Exchange or on the computer of the user.

If the user moves a secure message to an Outlook folder that is not synchronized with the Unity Connection Inbox folder, the only copy of the voice message is moved to the deleted items folder in Unity Connection, and the message can no longer be played in Outlook. If the user moves the message back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Unity Connection Inbox folder, and:

- If the message is still in the deleted items folder in Unity Connection, the message is synchronized back into the Unity Connection Inbox for that user, and the message becomes playable again in Outlook.
- If the message is not still in the deleted items folder in Unity Connection, the message is not resynchronized into Unity Connection and can no longer be played in Outlook.

How Message Routing Works through SMTP Domain Name

Cisco Unity Connection uses SMTP domain name to route messages between digitally networked Connection servers and to construct the SMTP address of the sender on outgoing SMTP messages. For each user, Unity Connection creates an SMTP address of <Alias>@<SMTP Domain>. This SMTP address is displayed on the Edit User Basics page for the user. Examples of outgoing SMTP messages that use this address format include messages sent by users on this server to recipients on other digitally networked Unity Connection servers and messages that are sent from the Unity Connection phone interface or Messaging Inbox and relayed to an external server based on the Message Actions setting of the recipient.

Unity Connection also uses the SMTP Domain to create sender VPIM addresses on outgoing VPIM messages, and to construct the From address for notifications that are sent to SMTP notification devices.

When Unity Connection is first installed, the SMTP Domain is automatically set to the fully qualified host name of the server.

Make sure that the SMTP domain of Cisco Unity Connection is different from the Corporate Email domain to avoid issues in message routing for Cisco Unity Connection.

Some scenarios in which you may encounter issues with the same domain are listed below:

- Routing of the voice messages between digitally networked Unity Connection servers
- Relaying of the messages
- Replying and Forwarding of the voice messages using ViewMail for Outlook
- Routing of the SpeechView messages to Cisco Unity Connection server
- Sending the SMTP message Notifications
- Routing of the VPIM messages

Note Cisco Unity Connection requires a unique SMTP domain for every user, which is different from the corporate email domain. Due to same domain name configuration on Microsoft Exchange and Cisco Unity Connection, the users who are configured for Unified Messaging may face issues in adding recipient while composing, replying and forwarding of messages.For more information on resolving domain name configuration issues, see the Resolving SMTP Domain Name Configuration Issues, page 2-47 section.

Where Deleted Messages Go

By default, when a user deletes a voice message in Unity Connection, the message is sent to the Unity Connection deleted items folder and synchronized with the Outlook Deleted Items folder. When the message is deleted from the Unity Connection deleted items folder (the user can do this manually, or you can configure message aging to do it automatically), it is also deleted from the Outlook Deleted Items folder.

If you are adding the single-inbox feature to an existing system, and if you have configured Unity Connection to permanently delete messages without saving them in the deleted items folder, messages that users delete by using the Web Inbox or by using the Unity Connection phone interface are still permanently deleted. However, messages that users delete by using Outlook are only moved to the Deleted Items folder in Outlook, not permanently deleted. When Unity Connection synchronizes with Exchange, the message is moved to the Unity Connection deleted items folder; it is not permanently deleted. We recommend that you do one or both of the following:

- Configure message aging to permanently delete messages in the Unity Connection deleted items folder.
- Configure message quotas, so that Unity Connection prompts users to delete messages when their mailboxes approach a specified size.

When a user deletes a voice message from any Outlook folder, including the Outlook Inbox folder, the Deleted Items folder, or any subfolder, the message is moved to the deleted items folder in Unity Connection. No operation in Outlook will cause a message to be permanently deleted in Unity Connection.

Types of Unity Connection Messages that are Not Synchronized with Exchange

The following types of messages are not synchronized:

- Draft messages
- Messages configured for future delivery but not yet delivered
- Broadcast messages
- Unaccepted dispatch messages. When a dispatch message has been accepted by a recipient, it becomes a normal message and is synchronized with Exchange for the user who accepted it and deleted for all other recipients. Until someone on the distribution list accepts a dispatch message, the message waiting indicator for everyone on the distribution list will remain on, even when users have no other unread messages.

Replication of Status Changes

Status changes (for example, from unread to read), changes to the subject line, and changes to the priority are replicated from Unity Connection to Exchange and vice versa, as applicable.

How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes

When you configure unified messaging, you create one or more unified messaging services that define, among other things, which unified messaging features are enabled. You also create one or more unified messaging accounts for each user to associate the user with unified messaging services. You can disable single inbox in three ways:

- Entirely disable a unified messaging service in which single inbox is enabled. This disables all enabled unified messaging features (including single inbox) for all users that are associated with the service.
- Disable only the single inbox feature for a unified messaging service, which disables only the single inbox feature for all users that are associated with that service.
- Disable single inbox for a unified messaging account, which disables single inbox only for the associated user.

If you disable and later re-enable single inbox by using any of these methods, Connection resynchronizes the Connection and Exchange mailboxes for the affected users. Note the following:

- If users delete messages in Exchange but do not delete the corresponding messages in Connection while single inbox is disabled, the messages will be resynchronized into the Exchange mailbox when single inbox is re-enabled.
- If messages are hard deleted from Exchange (deleted from the Deleted Items folder) before single inbox is disabled, the corresponding messages that are still in the deleted items folder in Unity Connection when single inbox is re-enabled will be resynchronized into the Exchange Deleted Items folder.
- If users delete messages in Connection but do not delete the corresponding messages in Exchange while single inbox is disabled, the messages remain in Exchange when single inbox is re-enabled. Users must delete the messages from Exchange manually.
- If users change the status of messages in Exchange (for example, from unread to read) while single inbox is disabled, the status of Exchange messages will be changed to the current status of the corresponding Connection messages when single inbox is re-enabled.
- When you re-enable single inbox, depending on the number of users associated with the service and the size of their Connection and Exchange mailboxes, resynchronization for existing messages may affect synchronization performance for new messages.

How Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts Are Synchronized

Unity Connection can send heard/read receipts, delivery receipts, and non-delivery receipts to Unity Connection users who send voice messages. If the sender of a voice message is configured for single inbox, the applicable receipt is sent to the Unity Connection mailbox for the sender. The receipt is then synchronized into the Exchange mailbox for the sender.

Note the following.

- *Read/heard receipts:* When sending a voice message, a sender can request a read/heard receipt. If you do not want Unity Connection to respond to requests for read receipts, in Connection Administration, uncheck the Respond to Requests for Read Receipts check box, which appears on the Users > Users > Edit > Mailbox page and on the Templates > User Templates > Edit > Mailbox page.

- *Delivery receipts:* A sender can request a delivery receipt only when sending a voice message from ViewMail for Outlook. You cannot prevent Unity Connection from responding to a request for a delivery receipt.
- *Non-delivery receipts (NDR):* A sender receives an NDR when a voice message cannot be delivered. If you do not want Unity Connection to send an NDR when a message cannot be delivered, in Connection Administration, uncheck the Send Non-Delivery Receipts for Message Failed Delivery check box, which appears on the Users > Users > Edit User Basics page and on the Templates > User Templates > Edit User Template Basics page.

  Note the following about NDRs:

  - When the sender accesses Unity Connection by using the TUI, the NDR includes the original voice message, which allows the sender to resend the message at a later time or to a different recipient.
  - When the sender accesses Unity Connection by using Web Inbox, the NDR includes the original voice message, but the sender cannot resend it.
  - When the sender uses ViewMail for Outlook to access Unity Connection voice messages that have been synchronized into Exchange, the NDR is a receipt that contains only an error code, not the original voice message, so the sender cannot resend the voice message.
  - When the sender is an outside caller, NDRs are sent to Unity Connection users on the Undeliverable Messages distribution list. Verify that the Undeliverable Messages distribution list includes one or more users who regularly monitors and reroutes undelivered messages.

Task List for Configuring Cisco Unity Connection and Exchange for Unified Messaging

To configure one or more unified messaging features, complete the following tasks in the order presented.

1. Review the "Requirements for Using Unified Messaging Features" section in the *System Requirements for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html .
2. *Cisco Unified Communications Manager Business Edition only:* Confirm that Unity Connection is licensed for single inbox. See the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section on page 2-17.
3. *If Unity Connection is integrated with an LDAP directory:* Review the current LDAP directory configurations to confirm that the Cisco Unified Communications Manager Mail ID field is synchronized with the LDAP mail field. During the integration process, this causes values in the LDAP mail field to appear in the Corporate Email Address field in Unity Connection.

   Unified messaging requires that you enter the Exchange email address for each Unity Connection user. On the Unified Messaging Account page, each user can be configured to use either of the following values:

   - The Corporate Email Address specified on the User Basics page
   - The email address specified on the Unified Messaging Account page

   Automatically populating the Corporate Email Address field with the value of the LDAP mail field is easier than populating the email address field on the Unified Messaging Account page by using Connection Administration or the Bulk Administration Tool.

If the Cisco Unified CM Mail ID field is synchronized with the sAMAccountName instead of the mail field, consider changing the LDAP directory configurations. For more information, see the "Changing LDAP Directory Configurations in Cisco Unity Connection 9.x" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter in the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

4. *If you are using single inbox and you want users to be able to use ViewMail for Outlook to send new voice messages, or to forward or reply to voice messages:* Install Cisco Unity Connection ViewMail for Microsoft Outlook on user workstations. For more information on installing ViewMail for Outlook, see the *Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook Release 8.5(x)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
5. Decide whether you want Unity Connection to communicate with a specific Exchange 2013, Exchange 2010 or Exchange 2007 client access server or Exchange 2003 server, or you want Unity Connection to be able to search for and communicate with different Exchange servers as required. See the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section on page 2-17.

   When you are using Exchange 2013, Exchange 2010 and/or Exchange 2007, Unity Connection searches for Exchange servers as described in *White Paper: Exchange 2007 Autodiscover Service*, available on the Microsoft website.

Note Unity Connection determines whether to use the HTTP or HTTPS protocol and whether to validate certificates based on settings in the applicable unified messaging service.

6. If you decided in Task 5. to allow Unity Connection to search for and communicate with different Exchange servers as required, and if Unity Connection is not already configured to use DNS, use the following CLI commands to configure DNS:
   - set network dns
   - set network dns options

   We recommend that you configure Unity Connection to use the same DNS environment in which the Active Directory environment is publishing its records.

   For more information on the CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
7. Confirm that all of the Exchange servers that Unity Connection will access are configured to use the desired authentication mode (basic, digest, or NTLM) and web-based protocol (HTTPS or HTTP). See the "Confirming Exchange Authentication and SSL Settings for Cisco Unity Connection" section on page 2-20.

Note If you want to configure SSL to encrypt the communication between Unity Connection and Exchange, configure Exchange to use HTTPS for the web-based protocol.

8. Create an Active Directory account to be used for Unity Connection unified messaging services, and grant the account the applicable permissions. See the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection" section on page 2-28.

9. *If you are using Exchange 2013 and Later:* Configure EWS limits for the unified messaging users. See the "Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2013 and Later)" section on page 2-33.
10. *If you are using Exchange 2010 SP2 RU4 and Later:* Configure EWS limits for the unified messaging users. See the "Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2010 SP2 RU4 and Later)" section on page 2-34.
11. *If you are using Exchange 2010 SP2 RU3 and Earlier Releases:* Configure EWS limits for the unified messaging services account. See the "Configuring EWS Limits for the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2010 SP2 RU3 and Earlier Releases)" section on page 2-36.
12. *If you are using Exchange 2003:* Enable the WebDav service. See the "Enabling the WebDav Service on Exchange 2003 Servers for Cisco Unity Connection" section on page 2-37.
13. *If you are using single inbox and users do not already have added SMTP proxy addresses:* Add proxy addresses to Unity Connection user accounts. For more information, see the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
14. Update class of service settings as required:
    - Enable single inbox in one or more classes of service. For more information, see the "Single Inbox in Cisco Unity Connection" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

      Note that all users who are configured to use single inbox must be in a class of service in which single inbox is enabled.

      Cisco Unified Communications Manager Business Edition only: Unity Connection counts all users in a class of service in which single inbox is enabled as single inbox users even if they are not configured to use single inbox. For example, if a Unity Connection server is licensed for 200 single-inbox users, and if you have three classes of service in which single inbox is enabled, the total number of users assigned to those three classes of service cannot exceed 200 users. This is true even if you only configure 50 users to use single inbox.
    - Enable text-to-speech access to Exchange voice messages on one or more classes of service: check the Allow Access to Advanced Features check box on the applicable class of service page, and then check the Allow Access to Exchange Email by Using Text to Speech (TTS) check box.
15. *If classes of service for single-inbox users have Delete Messages Without Saving to Deleted Items Folder enabled:* We recommend that you configure message aging and/or message quotas. Otherwise, messages deleted from Outlook may never be permanently deleted from Unity Connection. For more information, see the "Synchronizing Voice Messages in Unity Connection and Exchange Mailboxes in Cisco Unity Connection (Single Inbox)" section on page 2-3.

    For more information on configuring message aging and message quotas for Unity Connection, see the "Controlling the Size of Mailboxes in Cisco Unity Connection 9.x" chapter in the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

16. Configure one or more Unity Connection unified messaging services. See the "Creating a Unified Messaging Service to Access Exchange from Cisco Unity Connection" section on page 2-37.
17. *Selected configurations:* In either or both of the following configurations, upload SSL certificates on the Unity Connection server to encrypt communication between Unity Connection and Exchange and between Unity Connection and Active Directory:
    - If you configured Exchange to use HTTPS in Task 7. and configured unified messaging services to validate certificates for Exchange servers in Task 16.
    - If you configured Unity Connection to search for and communicate with different Exchange servers, to use LDAPS to communicate with domain controllers, and to validate certificates for domain controllers in Task 16.

Caution When you allow Unity Connection to search for and communicate with different Exchange servers, Unity Connection communicates with Active Directory servers using Basic authentication. By default, the user name and password of the unified messaging services account and all other communication between the Unity Connection and Active Directory servers is sent in clear text. If you want this data to be encrypted, in Task 16. you must configure unified messaging services to communicate with Active Directory domain controllers by using the secure LDAP (LDAPS) protocol.

For more information, see the "Uploading CA Public Certificates for Exchange and Active Directory Servers to the Cisco Unity Connection Server" section on page 2-40.

18. Test the unified messaging services. See the "Testing Unified Messaging Services for Cisco Unity Connection" section on page 2-42.
19. Update Unity Connection user accounts:
    - *Single inbox and text to speech only:* Update user settings to assign each user for whom single inbox or text to speech is enabled to a class of service in which single inbox or text to speech is enabled. See the applicable chapter in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html: either "Modifying or Deleting Individual User Accounts in Cisco Unity Connection 9.x" or "Managing Cisco Unity Connection 9.x User Accounts in Bulk."
    - Create unified messaging accounts for Unity Connection users. See the "Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes" section on page 2-42.
    - If you configured message aging and/or message quotas in Task 15.: Configure user accounts as applicable.

      For information on changing message aging settings for individual users, see the "Message Aging in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

      For information on changing message quota settings for individual users, see the "Mailbox-Size Quotas in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

20. Test unified messaging accounts for Unity Connection users. See the "Testing Unified Messaging Accounts for Cisco Unity Connection" section on page 2-45.
21. Test the unified messaging configuration. See the following sections:
    - Viewing a Summary of the Configuration of Unified Messaging Accounts for Cisco Unity Connection, page 2-45
    - Testing System Configuration, Including Unified Messaging, with Exchange and Cisco Unity Connection, page 2-46
    - Testing Access to Exchange Calendars for Cisco Unity Connection, page 2-47
22. *If Unity Connection voice messages are automatically being moved to the Outlook Junk Items folder:* Change the Outlook configuration to add the sender of the voice message or the sender's domain to the safe sender's list. For more information, see Outlook Help.
23. To teach users how to use the Unity Connection calendar, refer them to the following:
    - For listing, joining, and scheduling meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucugphone.html.
    - For importing Exchange contacts, see the "Managing Your Personal Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.
    - For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/pctr/b_9xcucugpctr.html.

Task List for Configuring Existing Cisco Unity Connection Users for Unified Messaging

After you configure unified messaging by following the "Task List for Configuring Cisco Unity Connection and Exchange for Unified Messaging" section on page 2-12, do the following tasks when you want to add unified messaging features for existing users.

1. *Single inbox or TTS for Cisco Unified CMBE only:* Ensure that you have sufficient licenses for the additional users. See the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section on page 2-17.
2. *If you are using single inbox and you want users to be able to use ViewMail for Outlook to send new voice messages, or to forward or reply to voice messages:* Add proxy addresses to Unity Connection user accounts. For more information, see the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
3. Update Unity Connection user accounts:

- *Single inbox and text to speech only:* Update user settings to assign each user for which single inbox or text to speech is enabled to a class of service in which single inbox or text to speech is enabled. See the applicable chapter in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html: either "Modifying or Deleting Individual User Accounts in Cisco Unity Connection 9.x" or "Managing Cisco Unity Connection 9.x User Accounts in Bulk."
- Create unified messaging accounts for Unity Connection users. See the "Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes" section on page 2-42.
- If you configured message aging and/or message quotas in Task 15.: Configure user accounts as applicable.

  For information on changing message aging settings for individual users, see the "Message Aging in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

  For information on changing message quota settings for individual users, see the "Mailbox-Size Quotas in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

4. Test unified messaging accounts for Unity Connection users. See the "Testing Unified Messaging Accounts for Cisco Unity Connection" section on page 2-45.
5. *If Unity Connection voice messages are automatically being moved to the Outlook Junk Items folder:* Change the Outlook configuration to add the sender of the voice message or the domain of the sender to the safe sender's list. For more information, see Outlook Help.

Determining which Exchange Servers You Want Cisco Unity Connection to Communicate with

When you add a unified messaging service, which defines the communication between Unity Connection and Exchange, you can choose whether you want Unity Connection to communicate directly with a specific Exchange server or you want Unity Connection to search for Exchange servers. The choice you make determines which Exchange mailboxes Unity Connection can access:

- If you choose a specific Exchange 2003 server, Unity Connection can only access mailboxes on that Exchange server.
- If you choose a specific Exchange 2007 client access server, Unity Connection can access all Exchange 2007 mailboxes in the Exchange organization, but cannot access Exchange 2003, Exchange 2010, or Exchange 2013 mailboxes.
- If you choose a specific Exchange 2010 client access server, Unity Connection can access all Exchange 2010 and Exchange 2007 mailboxes in the Exchange organization, but cannot access Exchange 2013 and Exchange 2003 mailboxes.

- If you choose a specific Exchange 2013 client access server, Unity Connection can access all Exchange 2013, Exchange 2010 and Exchange 2007 mailboxes in the Exchange organization, but cannot access Exchange 2003 mailboxes.
- If you choose to allow Unity Connection to search for Exchange servers, then you need to select from the following two options:
  - Exchange 2007 and/or 2010: Unity Connection can access every mailbox in the Exchange organization consisting of Exchange 2007, Exchange 2010, and Exchange 2013.
  - Exchange 2003, 2007 and/or 2010: Unity Connection can access every mailbox in the Exchange organization consisting of Exchange 2003, Exchange 2007, and Exchange 2010. When the Exchange organization includes Exchange 2003 servers, Unity Connection always communicates directly with the Exchange back-end servers, it never communicates with Exchange front-end servers.
- If you choose to allow Unity Connection to search for Exchange servers, you need to give permissions to the Exchange servers.

Note the following:

- If you want to choose a specific Exchange server when you add a unified messaging service, you may need to add more than one unified messaging service to allow Unity Connection to access all of the mailboxes in the Exchange organization. Table 2-3 explains when you need to add more than one unified messaging service.

Table 2-3 Adding Unified Messaging Services Based on Versions of Exchange

Exchange Versions on Which You Have Mailboxes That You Want Unity Connection to Be Able to Access					
Exchange 2003	**Exchange 2007**	**Exchange 2010**	**Exchange 2013**	**Office 365**	**Create the Following Unified Messaging Services**
No	No	No	No	Yes	• One for Office 365 server that you want Unity Connection to be able to access.
No	No	Yes	Yes	No	• One for Exchange 2013. This service can also access Exchange 2010 mailboxes.
No	No	Yes	Yes	Yes	• One for Exchange 2013. This service can also access Exchange 2010 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access.
No	Yes	No	No	No	• One for Exchange 2007.
No	Yes	No	No	Yes	• One for Exchange 2007. • One for Office 365 server that you want Unity Connection to be able to access.
No	Yes	Yes	Yes	No	• One for Exchange 2013. This service can also access Exchange 2010 and 2007 mailboxes.
No	Yes	Yes	Yes	Yes	• One for Exchange 2013. This service can also access Exchange 2010 and 2007 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access.

Exchange Versions on Which You Have Mailboxes That You Want Unity Connection to Be Able to Access					
Exchange 2003	**Exchange 2007**	**Exchange 2010**	**Exchange 2013**	**Office 365**	**Create the Following Unified Messaging Services**
Yes	No	No	No	No	• One for each Exchange 2003 server that you want Unity Connection to be able to access.
Yes	No	No	No	Yes	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Office 365 server that you want Unity Connection to be able to access
Yes	No	Yes	Yes	No	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2013. This service can also access Exchange 2010 mailboxes.
Yes	No	Yes	Yes	Yes	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2013. This service can also access Exchange 2010 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access
Yes	Yes	No	No	No	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2007.
Yes	Yes	No	No	Yes	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2007. • One for Office 365 server that you want Unity Connection to be able to access
Yes	Yes	Yes	Yes	No	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2013. This service can also access Exchange 2010 or Exchange 2007 mailboxes.
Yes	Yes	Yes	Yes	Yes	• One for each Exchange 2003 server that you want Unity Connection to be able to access. • One for Exchange 2013. This service can also access Exchange 2010 or Exchange 2007 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access.

- If you choose to allow Unity Connection to search for Exchange servers, Unity Connection can automatically detect when you move mailboxes from one version of Exchange to another and can automatically update Unity Connection user settings.

- If you choose a specific Exchange server, Unity Connection can sometimes detect when you move mailboxes from one Exchange server to another, and can automatically access the Exchange mailbox in the new location. When Unity Connection cannot detect mailbox moves, you must manually update unified messaging services or unified messaging accounts:
  - *If you moved all of the Exchange mailboxes accessed by a unified messaging service:* Update the unified messaging service to access a different Exchange server.
  - *If you moved only some of the Exchange mailboxes accessed by a unified messaging service:* Update unified messaging account settings to use a unified messaging service that accesses mailboxes in the new location.

  Table 2-4 identifies when Unity Connection can and cannot automatically detect mailbox moves between Exchange servers. For information on updating Unity Connection user settings when Unity Connection cannot detect mailbox moves, see the "Moving Microsoft Exchange Mailboxes for Connection Users Who Are Configured for Unified Messaging" chapter.

Table 2-4 Choosing a Specific Exchange Server: When Unity Connection Can Detect Mailbox Moves Between Exchange Servers

	Unity Connection can automatically detect mailbox moves between the following Exchange versions								
If you choose a specific	**2003 and 2003**	**2003 and 2007**	**2003 and 2010**	**2007 and 2007**	**2007 and 2010**	**2010 and 2010**	**2007 and 2013**	**2010 and 2013**	**2013 and 2013**
Exchange 2003 server	No	No	No	No	No	No	No	No	No
Exchange 2007 server	No	No	No	Yes	No	No	No	No	No
Exchange 2010 server	No	No	No	Yes	Yes	Yes	No	No	No
Exchange 2013 server	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

- If Unity Connection is not configured to use DNS, you must choose a specific Exchange server. If this does not allow you to access all of the Exchange mailboxes in the organization as described earlier in this section, you must create more than one unified messaging service.
- If you choose a specific Exchange server and that server stops functioning, Unity Connection cannot access any Exchange mailboxes. If you choose to allow Unity Connection to search for Exchange servers and if the Exchange server that Unity Connection is currently communicating with stops functioning, Unity Connection searches for another Exchange server and begins accessing mailboxes through that server.

Confirming Exchange Authentication and SSL Settings for Cisco Unity Connection

Confirm that the Exchange servers that Unity Connection will access are configured to use the desired authentication mode (basic, digest, or NTLM) and web-based protocol (HTTPS or HTTP). For information on which Exchange servers Unity Connection will access, see the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section on page 2-17.

Later in the task list, you will create one or more Unity Connection unified messaging services, and select the same authentication mode and web-based protocol that you specify in Exchange when you do the applicable procedures in this section.

Do the procedure in the applicable section:

Confirming Exchange 2013 Authentication and SSL Settings for Cisco Unity Connection

To Confirm Exchange 2013 Authentication and SSL Settings for Cisco Unity Connection

Step 1 Decide which type of authentication (basic or NTLM) you want Unity Connection to use to sign in to Exchange 2013 client access servers. You must configure the following servers to use the same type of authentication:

- All Exchange 2013 client access servers.

Step 2 Decide whether you want the communication between Unity Connection and Exchange 2013 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on the following servers:

- All Exchange 2013 client access servers.

Step 3 Sign in to a server that has access to the same Exchange 2013 client access servers that Unity Connection has. Use an account that is a member of the local Administrators group.

Step 4 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 5 For the first Exchange 2013 client access server for which you want to confirm settings, in the left pane, expand **<servername> > Sites > Default Website > EWS**.

Step 6 Under Default Website, select **Autodiscover**.

Step 7 In the middle pane, in the IIS section, double-click **Authentication**.

Step 8 Confirm that the Status column says **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange client access servers. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Unity Connection supports only the following types of authentication:

- Basic
- NTLM

Step 9 If you changed any settings, in the right pane, select **Apply**.

Step 10 In the left pane, select **Autodiscover** again.

Step 11 In the middle pane, double-click **SSL Settings**.

Step 12 If the **Require SSL** check box is checked:

- When you create a unified messaging service in Unity Connection, you must choose HTTPS for the web-based protocol.

- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Step 13 If you changed any settings, in the right pane, select **Apply**.

Step 14 In the left pane, under Default Website, select **EWS**.

Step 15 In the middle pane, in the IIS section, double-click **Authentication**.

Step 16 Confirm that the Status column says **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange mailboxes. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Caution The unified messaging services account must use the same type of authentication for EWS that you specified for autodiscover in Step 8.

Unity Connection supports only the following types of authentication:

- Basic
- NTLM

Step 17 If you changed any settings, in the right pane, select **Apply**.

Step 18 In the left pane, select **EWS** again.

Step 19 In the middle pane, double-click **SSL Settings**.

Step 20 If the **Require SSL** check box is checked:

- You must choose HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Caution The unified messaging services account must use the same SSL settings for EWS that you specified for autodiscover in Step 12.

Step 21 If you changed any settings, in the right pane, select **Apply**.

Step 22 Repeat Step 5 through Step 22 for the other Exchange 2013 client access servers that Unity Connection can access.

Step 23 Close IIS Manager.

Confirming Exchange 2010 Authentication and SSL Settings for Cisco Unity Connection

To Confirm Exchange 2010 Authentication and SSL Settings for Cisco Unity Connection

Step 1 Decide which type of authentication (basic, digest, or NTLM) you want Unity Connection to use to sign in to Exchange 2010 client access servers. You must configure the following servers to use the same type of authentication:

- All Exchange 2010 client access servers.

- All Exchange 2007 client access servers, if there are Exchange 2007 mailboxes that you want Unity Connection to be able to access.
- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.

Step 2 Decide whether you want the communication between Unity Connection and Exchange 2010 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on the following servers:

- All Exchange 2010 client access servers.
- All Exchange 2007 client access servers, if there are Exchange 2007 mailboxes that you want Unity Connection to be able to access.
- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.

Step 3 Sign in to a server that has access to the same Exchange 2010 client access servers that Unity Connection has. Use an account that is a member of the local Administrators group.

Step 4 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 5 For the first Exchange 2010 client access server for which you want to confirm settings, in the left pane, expand **<servername> > Sites > Default Website**.

Step 6 Under Default Website, select **Autodiscover**.

Step 7 In the middle pane, in the IIS section, double-click **Authentication**.

Step 8 Confirm that the Status column says **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange client access servers. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Unity Connection supports only the following types of authentication:

- Basic
- Digest
- NTLM

Step 9 If you changed any settings, in the right pane, select **Apply**.

Step 10 In the left pane, select **Autodiscover** again.

Step 11 In the middle pane, double-click **SSL Settings**.

Step 12 If the **Require SSL** check box is checked:

- When you create a unified messaging service in Unity Connection, you must choose HTTPS for the web-based protocol.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Step 13 If you changed any settings, in the right pane, select **Apply**.

Step 14 In the left pane, under Default Website, select **EWS**.

Step 15 In the middle pane, in the IIS section, double-click **Authentication**.

Step 16 Confirm that the Status column says **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange mailboxes. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Caution The unified messaging services account must use the same type of authentication for EWS that you specified for autodiscover in Step 8.

Unity Connection supports only the following types of authentication:

- Basic
- Digest
- NTLM

Step 17 If you changed any settings, in the right pane, select **Apply**.

Step 18 In the left pane, select **EWS** again.

Step 19 In the middle pane, double-click **SSL Settings**.

Step 20 If the **Require SSL** check box is checked:

- You must choose HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Caution The unified messaging services account must use the same SSL settings for EWS that you specified for autodiscover in Step 12.

Step 21 If you changed any settings, in the right pane, select **Apply**.

Step 22 If you have installed Exchange 2010 Service Pack 1 or later, skip to Step 23.

If you have not installed Exchange 2010 Service Pack 1 or later, edit the Exchange web.config files for EWS and for autodiscovery to match the settings in IIS Manager:

- For EWS, see "Enable or Disable SSL on Exchange Web Services Virtual Directories" on the Microsoft Technet website. Search on the document title.
- No comparable document exists for autodiscovery, but you can use the applicable procedure in the EWS document to edit the web.config file in the \Exchange Server\V14\ClientAccess\Autodiscover directory.

Step 23 Repeat Step 5 through Step 22 for the other Exchange 2010 client access servers that Unity Connection can access.

Step 24 Close IIS Manager.

Confirming Exchange 2007 Authentication and SSL Settings for Cisco Unity Connection

To Confirm Exchange 2007 Authentication and SSL Settings for Cisco Unity Connection

Step 1 Decide which type of authentication (basic, digest, or NTLM) you want Unity Connection to use to sign in to Exchange 2007 client access servers. You must configure the following servers to use the same type of authentication:

- All Exchange 2007 client access servers.
- All Exchange 2010 client access servers, if there are Exchange 2010 mailboxes that you want Unity Connection to be able to access.
- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.

Step 2 Decide whether you want the communication between Unity Connection and Exchange 2007 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on the following servers:

- All Exchange 2007 client access servers.
- All Exchange 2010 client access servers, if there are Exchange 2010 mailboxes that you want Unity Connection to be able to access.
- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.

Step 3 Sign in to a server that has access to the same Exchange 2007 client access servers as Unity Connection has. Use an account that is a member of the local Administrators group.

Step 4 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 5 For the first Exchange 2007 server for which you want to confirm settings, in the left pane, expand **<servername> > Sites > Default Website**.

Step 6 Under Default Website, right-click **Autodiscover**, and select **Properties**.

Step 7 In the Autodiscover Properties dialog box, select the **Directory Security** tab.

Step 8 In the Authentication and Access Control section, select **Edit**.

Step 9 In the Authentication Methods dialog box, confirm that the check box is checked for the type of authentication that you want the unified messaging services account to use to find Exchange servers. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Unity Connection supports only the following types of authentication:

- Basic
- Digest
- NTLM

Step 10 Select **OK**.

Step 11 In the Secure Communications section, select **Edit**.

Step 12 In the Secure Communications dialog box, if the **Require Secure Channel (SSL)** check box is checked:

- You must choose HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Step 13 Select **OK** twice.

Step 14 In the left pane, under Default Website, right-click **EWS**, and select **Properties**.

Step 15 In the EWS Properties dialog box, select the **Directory Security** tab.

Step 16 In the Authentication and Access Control section, select **Edit**.

Step 17 In the Authentication Methods dialog box, confirm that the check box is checked for the type of authentication that you want the unified messaging services account to use to find Exchange servers. When you create a unified messaging services account, you will configure Unity Connection to use the same type of authentication.

Caution The unified messaging services account must use the same type of authentication for EWS that you specified for autodiscover in Step 9.

Unity Connection supports only the following types of authentication:

- Basic
- Digest
- NTLM

Step 18 Select **OK**.

Step 19 In the Secure Communications section, select **Edit**.

Step 20 In the Secure Communications dialog box, if the **Require Secure Channel (SSL)** check box is checked:

- You must choose HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Caution The unified messaging services account must use the same SSL settings for EWS that you specified for autodiscover in Step 12.

Step 21 Select **OK** twice.

Step 22 Repeat Step 5 through Step 21 for the other Exchange 2007 client access servers that Unity Connection can access.

Step 23 Close IIS Manager.

Confirming Exchange 2003 Authentication and SSL Settings for Cisco Unity Connection

To Confirm Exchange 2003 Authentication and SSL Settings for Cisco Unity Connection

Step 1 Decide which type of authentication (basic, digest, or NTLM) you want Unity Connection to use to sign in to Exchange 2003 servers.

If you are configuring Unity Connection to search for Exchange servers, you must configure the following servers to use the same type of authentication:

- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.
- All Exchange 2007 client access servers.

- All Exchange 2010 client access servers, if there are Exchange 2010 mailboxes that you want Unity Connection to be able to access.

If you are choosing specific Exchange servers, you do not need to configure all Exchange servers to use the same type of authentication. Each Exchange server is associated with a separate unified messaging service, so the Exchange authentication mode only needs to match the authentication mode for the corresponding unified messaging service.

Note If you are choosing a specific Exchange 2003 front-end server, you may need to use basic authentication. For more information, on the Microsoft website, see the "Authentication Mechanisms for HTTP" in the Exchange Server 2003 section of the TechNet Library.

Step 2 Decide whether you want the communication between Unity Connection and Exchange 2007 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on the following servers:

- All Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.
- All Exchange 2007 client access servers.
- All Exchange 2010 client access servers, if there are Exchange 2010 mailboxes that you want Unity Connection to be able to access.

Step 3 Sign in to a server that has access to the same Exchange 2003 servers as Unity Connection has. Use an account that is a member of the local Administrators group.

Step 4 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 5 For the first Exchange 2003 server for which you want to confirm settings, in the left pane, expand **<servername> > Web Sites > Default Website**.

Step 6 Under Default Website, right-click **Exchange**, and select **Properties**.

Step 7 In the Exchange Properties dialog box, select the **Directory Security** tab.

Step 8 In the Authentication and Access Control section, select **Edit**.

Step 9 In the Authentication Methods dialog box, confirm that the check box is checked for the type of authentication that you want the unified messaging services account to use to sign in to Exchange servers. When you create a unified messaging service, you will configure Unity Connection to use the same type of authentication.

Unity Connection supports only the following types of authentication:

- Basic
- Digest
- NTLM

Step 10 Select **OK**.

Step 11 In the Secure Communications section, select **Edit**.

Step 12 In the Secure Communications dialog box, if the **Require Secure Channel (SSL)** check box is checked:

- You must choose HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

Step 13 Select **OK** twice.

Step 14 Repeat Step 5 through Step 13 for the other Exchange 2003 servers that you want Unity Connection to be able to access.

Step 15 Close IIS Manager.

Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection

Unity Connection accesses Exchange mailboxes by using an Active Directory account called the unified messaging services account. After you create the account, you grant it the rights necessary for Unity Connection to perform operations on behalf of the user. For Exchange 2013, 2010, and 2007, operations are performed through Exchange Web Services (EWS). For Exchange 2003, operations are performed through WebDav. These operations include uploading messages into Exchange mailboxes, tracking changes to the messages in Exchange, updating the messages with changes made in Unity Connection, deleting messages in Exchange when the messages are deleted in Unity Connection, tracking when messages are deleted in Exchange so they can be moved to the deleted items folder in Unity Connection, and so on.

See the following sections:

- Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection, page 2-28
- Confirming that the Local Computer Account Is a Member of the Windows Authorization Access Group on Client Access Servers for Cisco Unity Connection (Exchange 2007 Only), page 2-29
- Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Exchange 2013 and Exchange 2010 Only), page 2-30
- Granting Rights to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2007 Only), page 2-31
- Granting Permissions to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2003 Only), page 2-32

Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection

1. Create one or more domain user accounts in the Active Directory forest that includes the Exchange servers with which you want Unity Connection to communicate. Note the following:
   - Give the account a name that identifies it as the unified messaging services account for Unity Connection.
   - Do not create an Exchange mailbox for the account.

Caution If you create a mailbox for the account, unified messaging will not function properly.

   - Do not add the account to any administrator group.

- Do not disable the account, or Unity Connection cannot use it to access Exchange mailboxes.
- Specify a password that satisfies the password-security requirements of your company.

  The password is encrypted with AES 128-bit encryption and stored in the Unity Connection database. The key that is used to encrypt the password is accessible only with root access, and root access is available only with assistance from Cisco TAC.
- When you are configuring unified messaging for a Unity Connection cluster, Unity Connection automatically uses the same unified messaging services account for both Unity Connection servers.
- When you are configuring unified messaging for intersite networking or for intrasite networking, you can use the same unified messaging services account for more than one Unity Connection server. However, this is not a requirement and does not affect functionality or performance.

2. *If you are using Exchange 2007:* For all client access servers, confirm that the local computer account is a member of the Windows Authorization Access group. See the "Confirming that the Local Computer Account Is a Member of the Windows Authorization Access Group on Client Access Servers for Cisco Unity Connection (Exchange 2007 Only)" section on page 2-29.
3. For each version of Exchange that you want Unity Connection to be able to access, do the procedure in the corresponding section:
   - Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Exchange 2013 and Exchange 2010 Only), page 2-30
   - Granting Rights to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2007 Only), page 2-31
   - Granting Permissions to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2003 Only), page 2-32

Confirming that the Local Computer Account Is a Member of the Windows Authorization Access Group on Client Access Servers for Cisco Unity Connection (Exchange 2007 Only)

If you are configuring unified messaging for Unity Connection users whose Exchange mailboxes are homed on Exchange 2007 servers, do the following procedure to confirm that the local computer accounts for those servers are members of the Windows Authorization Access group, as they are by default. Do the procedure for all Exchange 2007 client access servers that Unity Connection can access.

To Confirm that the Local Computer Account Is a Member of the Windows Authorization Access Group on Client Access Servers for Cisco Unity Connection (Exchange 2007 Only)

Step 1 Sign in to a server on which Active Directory Users and Computers is installed. Use an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, select Administrative Tools > Active Directory Users and Computers.

Step 3 In the left pane, expand the name of a domain that contains Exchange 2007 client access servers that Unity Connection can access, and select **Builtin**.

Step 4 In the right pane, right-click Windows Authorization Access Group, and select **Properties**.

Step 5 In the Windows Authorization Access Group Properties dialog box, select the **Members** tab.

Step 6 Select **Add**.

Step 7 In the Select Users, Contacts, Computers, or Groups dialog box, select **Object Types**.

Step 8 Check the **Computers** check box.

Step 9 Select **OK** to close the Object Types dialog box.

Step 10 On the Select Users, Contacts, Computers, or Groups dialog box, enter the names of all of the Exchange 2007 client access servers in the domain that you expanded in Step 3.

Step 11 Select **Check Names**.

Step 12 Select **OK** to close the Select Users, Contacts, Computers, or Groups dialog box.

Step 13 Select **OK** to close the Windows Authorization Access Group Properties dialog box.

Step 14 Repeat Step 3 through Step 13 for the other domains that contain Exchange 2007 client access servers that Unity Connection can access.

Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Exchange 2013 and Exchange 2010 Only)

To Assign the ApplicationImpersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Exchange 2013 and Exchange 2010 Only)

Step 1 Sign in to a server on which Exchange Management Shell is installed. Sign in by using either an account that is a member of the Enterprise Admins group or an account that has permission to grant permissions on Exchange objects in the configuration container.

Step 2 Run the following command in Exchange Management Shell to assign the ApplicationImpersonation management role to the unified messaging services account for Exchange 2013 and Exchange 2010.

new-ManagementRoleAssignment -Name:*RoleName* **-Role:ApplicationImpersonation -User:'***Account***'**

where:

- *RoleName* is the name that you want to give the assignment, for example, Unity ConnectionUMServicesAcct. The name that you enter for *RoleName* appears when you run get-ManagementRoleAssignment.
- *Account* is the name of the unified messaging services account in domain\alias format.

Step 3 If you created more than one unified messaging services account, repeat Step 2 for the remaining accounts. Specify a different value for *RoleName* for each unified messaging services account.

Note When configuring Unified Messaging service account for Exchange 2013 or Exchange 2010, you need to assign the ApplicationImpersonation management role to the Unified Messaging service account

Granting Rights to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2007 Only)

Do the following procedures for all unified messaging services accounts.

To Grant Rights to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2007 Only)

Step 1 Sign in to a server on which Exchange Management Shell is installed. Sign in by using either an account that is a member of the Enterprise Admins group or an account that has permission to grant rights on Exchange objects in the configuration container.

Step 2 Run the following commands in Exchange Management Shell to grant the required rights to the unified messaging services account for Exchange 2007:

Add-ADPermission -Identity (*PermissionLevel*)**.DistinguishedName -User (Get-User -Identity** *Account* **| select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation**

Add-ADPermission -Identity (*PermissionLevel*)**.DistinguishedName -User (Get-User -Identity** *Account* **| select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate**

Add-ADPermission -Identity (*PermissionLevel*)**.DistinguishedName -User (Get-User -Identity** *Account* **| select-object).identity -ExtendedRights Receive-As**

where:

- *PermissionLevel* is determined by whether you want to grant the unified messaging services account rights to access individual servers or rights to access all Exchange 2007 servers in the organization:
  - To grant the unified messaging services account rights to access individual Exchange servers, replace *PermissionLevel* with:

    Get-ExchangeServer -Identity *ServerName*

    where *ServerName* is the name of the Exchange 2007 server to which you want the unified messaging services account to have access.
  - To grant the unified messaging services account rights to access all Exchange 2007 servers in the Exchange organization, replace *PermissionLevel* with:

    Get-OrganizationConfig

  For more information on the Add-ADPermission commandlet and the Identity parameter, see Exchange 2007 Help.
- *Account* is the name of the unified messaging services account in domain\alias format.

Step 3 If you created more than one unified messaging services account, repeat Step 2 for the remaining accounts.

Step 4 If you set permissions on individual Exchange server in Step 2 and you have more than one Exchange 2007 server, repeat Step 1 through Step 3 on the following servers:

- All other Exchange 2007 client access servers that Unity Connection can access.
- All Exchange 2007 mailbox servers that home mailboxes that you want Unity Connection to be able to access.

To Grant Unified Messaging Services Accounts the Permission to Sign In Locally for Cisco Unity Connection (Exchange 2007 Only)

Step 1 On an Exchange 2007 client access server that Unity Connection can access, sign in by using an account that is a member of the local Administrators group.

Step 2 On the Windows Start menu, select **Administrative Tools > Local Security Policy**.

Step 3 In the left pane, expand **Local Policies**, and select **User Rights Assignment**.

Step 4 In the right pane, right-click **Allow Log on Locally**, and select **Properties**.

Step 5 In the Allow Log on Locally Properties dialog box, on the **Local Security Setting** tab, select **Add User or Group**.

Step 6 On the Select Users, Computers, or Groups dialog box, enter the name of the unified messaging services account that you created in Task 1. of the "Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection" section on page 2-28.

If intrasite networking or intersite networking is configured, and if you created more than one unified messaging services account, enter the names of the unified messaging services accounts for the Unity Connection servers that will access this Exchange 2007 client access server.

Step 7 Select **Check Names**.

Step 8 Select **OK** to close the Select Users, Computers, or Groups dialog box.

Step 9 Select **OK** to close the Allow Log on Locally Properties dialog box.

Step 10 Close Local Security Settings.

Step 11 Repeat Step 1 through Step 10 on the following servers:

- All other Exchange 2007 client access servers that Unity Connection can access.
- All Exchange 2007 mailbox servers that home mailboxes that you want Unity Connection to be able to access.

Granting Permissions to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2003 Only)

To grant permissions to the unified messaging services account so Unity Connection can access Exchange 2003, do the following procedure.

To Grant Permissions to the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2003 Only)

Step 1 Sign in to a server on which Exchange System Manager is installed. Sign in by using either an account that is a member of the Enterprise Admins group or an account that has permission to grant permissions on Exchange objects in the configuration container.

Step 2 On the Windows Start menu, select **Programs > Microsoft Exchange > System Manager**.

Step 3 In the left pane, expand **Servers**.

Step 4 Right-click the name of the Exchange server that contains mailboxes that will be accessed by Cisco Unity Connection, and select **Properties**.

Step 5 In the <Server name> Properties dialog box, select the **Security** tab.

Step 6 Select **Add**.

Step 7 In the Select Users, Computers, or Groups dialog box, in the Enter the Object Names to Select field, enter the name of the unified messaging services account.

Step 8 Select **Check Names**.

Step 9 Select **OK** to close the dialog box.

Step 10 In the <Server name> Properties dialog box, in the Group or User Names list, select the name of the unified messaging services account.

Step 11 In the Permissions For <Account name> list, check the **Allow** check box for the following permissions:

- **Send As**
- **Receive As**
- **Administer Information Store**

Step 12 Select **OK** to close the <Server name> Properties dialog box.

Step 13 Repeat Step 4 through Step 12 for each additional Exchange server that you want to access.

Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2013 and Later)

Revised September 10, 2013

If any unified users' Exchange mailboxes have more than 1000 messages, which includes voice messages and receipts, then enable the EWS paged view search functionality at Cisco Unity Connection. To enable the paged view functionality for messages, you must set the value of the 'System.Messaging.MbxSynch.MbxSynchUsePaging' parameter to 1.

Note In case you are using 9.1.2 ES2 and later, make sure to enable the paged view search functionality.For more information on how to enable the paged view functionality, see the "To Enable the Paged View Functionality, Perform the Following Steps" section on page 2-33 section of this guide.

To Enable the Paged View Functionality, Perform the Following Steps

Step 1 Run the following CLI command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchUsePaging',pvalue
=1)
```

Note When a Cisco Unity Connection cluster is configured, you can run the command on publisher or subscriber server.

Step 2 To set the maximum limit of voice messages items that can be managed by Cisco Unity Connection with the Paged view search functionality, run the following CLI command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pFullName='System.Messaging.MbxSynch.MbxSynchVoiceMailCountLimit',
pvalue="newvalue")
```

where, new value specifies the value of the voicemails count limit that you can view after the paging parameter is enabled. Cisco Unity Connection by default manages the first 25000 voice messages per mailbox that avoid any delay in message synchronization between Unity Connection and Exchange server. This voicemail count limit can be increased maximum up to 75000.

Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2010 SP2 RU4 and Later)

Revised September 10, 2013

Microsoft has enabled the client throttling policy feature by default. If there is no throttling policy already configured, Microsoft Exchange applies a default policy to all users. The default throttling policy is tailored for end user's load and not for an enterprise application like, Cisco Unity Connection using impersonation. If any Cisco Unity Connection users who are configured for unified messaging have mailboxes in Exchange 2010, configure the Exchange 2010 EWS limits for the unified messaging users mailbox by creating and applying a new mailbox policy to the unified messaging user mailbox account. If you do not configure EWS limits, messages may not be synchronized, and status changes (for example, from unread to read), changes to the subject line, and changes to the priority may not be replicated. In addition, attempts to access Exchange calendars and contacts may fail.

Note After Exchange 2010 SP2 RU4, when Exchange impersonation is used, the budgets for all the throttling thresholds calculated against the account that is impersonated (target mailbox) and not the impersonating account (Unified Messaging Service Account).

Note In case you are using 9.1.2 ES2 and later, make sure to enable the paged view search functionality.For more information on how to enable the paged view functionality, see the "To Enable the Paged View Functionality, Perform the Following Steps" section on page 2-33 section of this guide. If you have the paged view search functionality disabled or using Unity Connection versions previous to 9.1.2 ES2 version, configure the EWS limits for affected unified users by following the below given steps.

To Configure EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2010 Service Pack 2 RU4 and Later)

Step 1 Sign in to a server on which Exchange Management Shell is installed. Sign in by using either an account that is a member of the Enterprise Admins group or an account that has permission to grant permissions on Exchange objects in the configuration container.

Step 2 Create a new policy with the following EWS connections where Exchange mailboxes have more than 1000 messages, which includes voice messages and receipts. For Exchange mailboxes having 10000 messages, then the new throttling policy will be:

New-ThrottlingPolicy -Name "<*ConnectionUnifiedMessagingServicesPolicy*>" -EWSPercentTimeInCAS 300 -EWSPercentTimeInMailboxRPC 200 -EWSFindCountLimit 10000 -EWSPercentTimeinAD 100

where *ConnectionUnifiedMessagingServicesPolicy* is the name that you want to assign to the policy. Refer to the Table 2-5 to have detailed description on the throttling policy parameters.

Step 3 Apply the new policy to all the unified messaging user mailbox. For each user mailbox, run the following command:

Set-ThrottlingPolicyAssociation -Identity "<*ConnectionUnifiedMessagingusermailbox*>**" -ThrottlingPolicy "**<*ConnectionUnifiedMessagingServicesPolicy*>**"**

where:

- *ConnectionUnifiedMessagingusermailbox* is the name of the user mailbox.
- *ConnectionUnifiedMessagingServicesPolicy* is the name of the policy that you created in Step 2.

Step 4 Confirm that the mailbox is using the new policy:

Get-ThrottlingPolicyAssociation -Identity "<*ConnectionUnifiedMessagingusermailbox*>**" | findstr "ThrottlingPolicy"**

Step 5 On each Exchange 2010 server that has the CAS role, restart the Microsoft Exchange RPC Client Access service.

Table 2-5 Recommended Throttle Policy Parameter Values With 10000 Items in User's Mailbox

Field	Policy Value To Be Used	Description
EWSPercentTimeInCAS	300	Specifies the percentage of a minute that an Exchange Web Services user can spend executing the client access server code (PercentTimeInCAS).
EWSPercentTimeInMailboxRPC	200	Specifies the percentage of a minute that an Exchange Web Services user can spend executing mailbox remote procedure call (RPC) requests (PercentTimeInMailboxRPC).
EWSFindCountLimit	10000	Defines the maximum number of items from a FindItem or FindFolder operation that can exist in memory on the Client Access server at one time for one user. **Note** If in your deployment mailboxes have more than 10,000 messages, then you can adjust this parameter.
EWSPercentTimeinAD	100	Specifies the maximum amount of time that can be spent by a Client Access server when accessing Active Directory resources on behalf of a client account, per minute.

Configuring EWS Limits for the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2010 SP2 RU3 and Earlier Releases)

Revised September 10, 2013

If any Unity Connection users who are configured for unified messaging have mailboxes in Exchange 2010, configure the Exchange 2010 EWS limits for the unified messaging service account by creating and applying a new mailbox policy to the unified messaging services account. If you do not configure EWS limits, messages may not be synchronized, and status changes (for example, from unread to read), changes to the subject line, and changes to the priority may not be replicated. In addition, attempts to access Exchange calendars and contacts may fail.

Note Prior to Exchange 2010 Service Pack 1, EWS limits were off by default. If you have not yet installed Service Pack 1, which turns limits on by default, we still recommend that you do the following procedure. Otherwise, when you install Service Pack 1, Unity Connection functionality will be affected.

To Configure EWS Limits for the Unified Messaging Services Account for Cisco Unity Connection (Exchange 2010 SP2 RU3 and Earlier Releases)

Step 1 Sign in to a server on which Exchange Management Shell is installed. Sign in by using either an account that is a member of the Enterprise Admins group or an account that has permission to grant permissions on Exchange objects in the configuration container.

Step 2 Create a new policy with unlimited EWS connections:

New-ThrottlingPolicy -Name "<*ConnectionUnifiedMessagingServicesPolicy*>**" -EWSMaxConcurrency $null -EWSMaxSubscriptions $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null -EWSFindCountLimit $null -EWSPercentTimeinAD $null**

where *ConnectionUnifiedMessagingServicesPolicy* is the name that you want to assign to the policy.

Step 3 Apply the new policy to the unified messaging services account and the user mailbox:

Set-ThrottlingPolicyAssociation -Identity "<*ConnectionUnifiedMessagingServicesAccount*>**" -ThrottlingPolicy "**<*ConnectionUnifiedMessagingServicesPolicy*>**"**

where:

- *ConnectionUnifiedMessagingServicesAccount* is the name of the account that you created in the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection" section on page 2-28.
- *ConnectionUnifiedMessagingServicesPolicy* is the name of the policy that you created in Step 2.

Note The Set-ThrottlingPolicyAssociation command is not supported with Exchange 2010 version 14.00.0639.021. The users having Exchange 2010 with version 14.00.0639.021 are not allowed to modify an existing throttling policy settings, hence the default policy gets applied here.

Step 4 Confirm that the mailbox is using the new policy:

Get-ThrottlingPolicyAssociation -Identity "<*ConnectionUnifiedMessagingServicesAccount*>**" | findstr "ThrottlingPolicy"**

Step 5 If you created more than one unified messaging services account, repeat Step 3 and Step 4 for the remaining accounts.

Step 6 On each Exchange 2010 server that has the CAS role, restart the Microsoft Exchange RPC Client Access service.

Enabling the WebDav Service on Exchange 2003 Servers for Cisco Unity Connection

If you want Unity Connection to access mailboxes on Exchange 2003 servers, you need to configure Internet Information Services to allow the WebDav service. Do the following procedure.

To Enable the WebDav Service on Exchange 2003 for Cisco Unity Connection

Step 1 Sign in to a server that has access to the same Exchange 2003 servers that the Unity Connection server has access to. Use an account that is a member of the local Administrators group.

Step 2 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 3 For the first Exchange 2003 server for which you want to confirm settings, in the left pane, expand **<servername>** and select **Web Service Extensions**.

Step 4 In the right pane, for WebDAV, check the value of the Status column:

- If the value is Allowed, skip to Step 5.
- If the value is Prohibited, select **Allow**.

Step 5 Repeat Step 3 and Step 4 for the other Exchange 2003 servers that you want Unity Connection to be able to access.

Step 6 Close IIS Manager.

Creating a Unified Messaging Service to Access Exchange from Cisco Unity Connection

Do the following procedure to create one or more unified messaging services.

To Create a Unified Messaging Service to Access Exchange from Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging**, then select **Unified Messaging Services**.

Step 2 On the Search Unified Messaging Services page, select **Add New**.

Step 3 Decide which options to select for the **Message Action for Email** and **Message Action for Fax** lists at the bottom of the page. (For field information, on the Help menu, select **This Page**.)

If you want to select **Relay the Message** or **Accept and Relay the Message** for either list, you must first configure an SMTP Smart Host on the **System Settings > SMTP Configuration > Smart Host** page. Connection Administration will not let you save a new unified messaging configuration with those settings when no SMTP Smart Host is configured.

Step 4 On the New Unified Messaging Service page, in the Type list, select **Exchange/BPOS -D**.

Step 5 Check the **Enabled** check box to enable the service.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes" section on page 2-11.

Step 6 In the Display Name field, enter a descriptive name.

If you are creating more than one unified messaging service for Exchange, note that this is the name that will appear on the Users > Unified Messaging Accounts page when you configure users for unified messaging. Enter a display name that will simplify choosing the correct unified messaging service for each user.

Step 7 In the **Web-Based Authentication Mode** list, select the same authentication mode that you confirmed when you did the applicable procedures in the "Confirming Exchange Authentication and SSL Settings for Cisco Unity Connection" section on page 2-20.

Step 8 In the **Web-Based Protocol** list, select the same web-based protocol that you confirmed when you did the applicable procedures in the "Confirming Exchange Authentication and SSL Settings for Cisco Unity Connection" section on page 2-20.

Step 9 If you want Unity Connection to validate the SSL certificate from the Exchange server, check the **Validate Certificates for Exchange Servers** check box.

Self-signed certificates cannot be validated. If you selected **HTTPS** from the **Web-Based Protocol** list, and if you are using self-signed certificates, do not check the **Validate Certificates for Exchange Servers** check box. If you do check the check box, Unity Connection will not be able to access Exchange.

Step 10 In the Exchange servers section, if you want Unity Connection to access a specific Exchange server, skip to Step 11.

If you want Unity Connection to automatically find Exchange 2013, Exchange 2010, or Exchange 2007 client access servers, or Exchange 2003 servers, do the following:

a. Select **Search for Exchange Servers**.

b. In the Active Directory DNS Domain Name field, enter the DNS domain name of the Active Directory domain in which you want Unity Connection to begin searching for Exchange servers.

c. If you have Exchange servers in more than one Active Directory site, you can improve performance if you specify the site that contains the domain controllers that you want Unity Connection to use to find Exchange servers. In the **Active Directory Site Name** field, enter the name of the site.

d. Under Exchange Versions, select the versions of Exchange in which you have mailboxes that you want Unity Connection to be able to access.

e. In the **Protocol Used to Communicate with Domain Controllers** list, select whether Unity Connection should use LDAP or secure LDAP (LDAPS) when communicating with Active Directory to find Exchange servers.

Caution When you select **Search for Exchange Servers**, Unity Connection communicates with Active Directory servers using Basic authentication regardless of the authentication method you selected in the **Web-Based Authentication Mode** list. As a result, the username and password of the unified messaging services account and all other communication between the Unity Connection and Active Directory servers is in clear text. If you want this data to be encrypted, you must select Secure LDAP (LDAPS) in the **Protocol Used to Communicate with Domain Controllers** list and upload certificates from the certification authority that issued the SSL certificates for Active Directory servers to both tomcat-trust and Connection-trust locations. See Task 17. in the "Task List for Configuring Cisco Unity Connection and Exchange for Unified Messaging" section on page 2-12.

f. If you want Unity Connection to validate the SSL certificate from Active Directory domain controllers, check the **Validate Certificates for Active Directory Domain Controllers** check box.

   Self-signed certificates cannot be validated. If you selected **LDAPS** from the **Protocol Used to Communicate with Domain Controllers** list, and if you are using self-signed certificates, do not check the **Validate Certificates for Active Directory Domain Controllers** check box. If you do check the check box, Unity Connection will not be able to access domain controllers to search for Exchange servers.

g. Skip to Step 12.

Step 11 To configure Unity Connection to access a specific Exchange server, do the following:

a. Select **Specify an Exchange Server**.

b. In the **Exchange Server** field, enter the fully qualified domain name or the IP address of the Exchange server that you want Unity Connection to access. If you are entering the name of an Exchange 2013, Exchange 2010, or Exchange 2007 CAS server, you must enter the name of a client access server.

c. In the **Exchange Server Type** list, select the version of Exchange installed on the server that you specified in Step b.

Step 12 In the Username and Password fields, enter the Active Directory username and password for the account that you created in the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection" section on page 2-28.

If you specify the username in domain\username format, do not use FQDN format for the domain name.

Step 13 Under Service Capabilities, select the features that you want this unified messaging service to allow.

Note When you configure unified messaging for Unity Connection users, you can disable for an individual user any feature that you enable here. However, you cannot enable for an individual user any feature that you disable here.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes" section on page 2-11.

Step 14 Under Synchronize Connection and Exchange Mailboxes (Single Inbox), choose message actions for email and for fax. (For field information, on the Help menu, select This Page.)

Step 15 Select **Save**.

Note If you selected **HTTPS** in the Web-Based Protocol list, or if you selected **Secure LDAP (LDAPS)** in the **Protocol Used to Communicate with Domain Controllers** list, you cannot test the configuration until after you have uploaded SSL certificates in Task 17. of the "Task List for Configuring Cisco Unity Connection and Exchange for Unified Messaging" section on page 2-12 because the security-related tests will fail.

Step 16 If you are configuring Unity Connection to communicate with individual Exchange servers, repeat Step 2 through Step 15 to create additional unified messaging services as explained in the "Determining Which Exchange Servers You Want Cisco Unity Connection to Communicate With" section on page 2-17.

Uploading CA Public Certificates for Exchange and Active Directory Servers to the Cisco Unity Connection Server

When you created unified messaging services, if you selected the option to validate certificates for Exchange servers or for Active Directory domain controllers (DCs), you must upload the public certificates from the certification authority (CA) that signed the certificates on the Exchange servers and DCs. Otherwise, Unity Connection cannot communicate with Exchange servers or with DCs to find Exchange servers, and unified messaging functionality will not work. Do the following tasks:

1. *If you selected the option to validate certificates for Exchange servers, and if SSL certificates are not already installed on all of the following servers:* Get and install certificates:
   - Exchange 2013 or Exchange 2010 client access servers.
   - Exchange 2007 client access servers, if there are Exchange 2007 mailboxes that you want Unity Connection to be able to access.
   - Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.

   In addition, if you selected the option to validate certificates for Active Directory domain controllers, and if SSL certificates are not already installed on your DCs, get and install certificates.
2. *If you used an external CA (for example, Verisign) to issue the SSL certificates installed on the servers listed in Task 1., and if you have the public certificates for the CA in .pem format:* Save the files to a network location accessible to the Unity Connection server. Then skip to Task 6.
3. *If you used Microsoft Certificate Services or Active Directory Certificate Services to issue the SSL certificates, or if you used an external CA and you do not have the public certificate for the CA in .pem format:* Download and install OpenSSL or another application that can convert public certificates to .pem format. Unity Connection cannot upload public certificates in other formats.
4. *If you used Microsoft Certificate Services to issue the SSL certificates:* Do the "To Save the Public Certificate for Microsoft Certificate Services or Active Directory Certificate Services to a File" section on page 2-41.
5. *If you used Microsoft Certificate Services, Active Directory Certificate Services, or an external CA, and if you do not have public certificates in .pem format:* Use the application that you downloaded in Task 3. to convert the public certificate to .pem format, and save the file to a network location accessible to the Unity Connection server.

6. Upload the public certificates to the Unity Connection server. See the "To Upload the Public Certificates to the Unity Connection Server" procedure on page 2-41.

To Save the Public Certificate for Microsoft Certificate Services or Active Directory Certificate Services to a File

Step 1 Sign in to the server on which you installed Microsoft Certificate Services and issued SSL certificates for the following servers:

- Exchange 2013 or Exchange 2010 client access servers.
- Exchange 2007 client access servers, if there are Exchange 2007 mailboxes that you want Unity Connection to be able to access.
- Exchange 2003 servers, if any, on which there are mailboxes that you want Unity Connection to be able to access.
- Active Directory domain controllers that the Unity Connection server might access.

Step 2 On the Windows Start menu, select **Programs > Administrative Tools > Certification Authority**.

Step 3 In the left pane of the Certification Authority MMC, right-click the server name, and select **Properties**.

Step 4 In the <servername> Properties dialog box, on the General tab, select **View Certificate**.

Step 5 In the Certificate dialog box, select the **Details** tab.

Step 6 On the Details tab, select **Copy to File**.

Step 7 On the Welcome to the Certificate Export Wizard page, select **Next**.

Step 8 On the Export File Format page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.

Step 9 On the File to Export page, specify the full path of the public certificate, including a location that is accessible to the Unity Connection server, and a file name.

Step 10 Select **Next**.

Step 11 On the Completing the Certificate Export Wizard page, select **Finish**.

Step 12 Select **OK** three times to close a message box and two dialog boxes.

Step 13 Close the Certification Authority MMC.

Step 14 If you issued SSL certificates for all of the servers listed in Step 1 by using the same installation of Microsoft Certificate Services, you are finished with this procedure. Return to the task list for this section.

If you issued SSL certificates for all of the servers listed in Step 1 by using different installations of Microsoft Certificate Services, repeat Step 1 through Step 13 to get one public certificate for each instance of Microsoft Certificate Services. Then return to the task list for this section.

To Upload the Public Certificates to the Unity Connection Server

Step 1 On the Unity Connection server, sign in to Cisco Unified Operating System Administration.

Step 2 On the Security menu, select **Certificate Management**.

Step 3 Select **Upload Certificate**.

Step 4 In the Certificate Name list, select **tomcat-trust**.

Step 5 *Optional:* Enter a description (for example, the name of the certification authority) in the Description field.

Step 6 Select **Browse**.

Step 7 Browse to the location where you saved the public certificates in .pem format, and select one of the converted certificates.

Step 8 Select **Upload File**.

Step 9 Repeat Step 3 through Step 8, but select **Unity Connection-trust** in the Certificate Name list.

Step 10 If you have public certificates from more than one certification authority, repeat Step 3 through Step 9 for the remaining certificates.

Testing Unified Messaging Services for Cisco Unity Connection

Do the following procedure to test one or more unified messaging services.

To Test Unified Messaging Services for Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging**, then select **Unified Messaging Services**.

Step 2 On the Search Unified Messaging Services page, select the service that you want to test.

Step 3 On the Edit Unified Messaging Service page, select **Test**.

Step 4 If the test results showed configuration problems, resolve the problems, then repeat the test.

Step 5 If you configured two or more unified messaging services, repeat Step 1 through Step 4 to test the remaining services.

Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes

This section contains the following sections:

How Unified Messaging Accounts and User Accounts are Related for Cisco Unity Connection

Unified messaging accounts tie Unity Connection users to unified messaging services. Unified messaging accounts are separate objects from user accounts:

- When you create a user account, Unity Connection does not automatically create a unified messaging account for that user.
- You can create more than one unified messaging account for a user, but a user's unified messaging accounts cannot have overlapping features. For example, you cannot create two unified messaging accounts for the same user that both enable single inbox.

  Creating multiple unified messaging accounts for a user is one way to control access to unified messaging features. For example, if you want all users to have single inbox but only a few users to have text-to-speech access to Exchange email, you can create two unified messaging services. One activates single inbox and the other activates TTS. You then create unified messaging accounts for all users to give them access to single inbox, and you create a second unified messaging account for the users who you want to have TTS.
- When you add a unified messaging account, the associated user account is updated with a reference to the unified messaging account. The user account does not contain the information on the unified messaging account.
- When you delete a user account, all unified messaging accounts for that user are also deleted. However, when you delete a unified messaging account, the corresponding user account is not deleted. The user account is updated only to remove the reference to the unified messaging account.

Creating Unified Messaging Accounts for Cisco Unity Connection

Do the following procedure to create one or more unified messaging accounts for Unity Connection users by using Connection Administration. You can also create large numbers of unified messaging accounts by using the Bulk Administration Tool. For more information, see the "Using the Cisco Unity Connection 9.x Bulk Administration Tool" appendix in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Note Each unified messaging account is associated with a user, but a unified messaging account is a separate object in the Unity Connection database. If you delete a unified messaging account, the associated user account is not deleted.

To Create Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user.

Note If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

Step 3 On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4 On the Unified Messaging Accounts page, select **Add New**.

Step 5 On the New Unified Messaging Account page, in the Unified Messaging Service list, select the name of the service that you want to use for this user. You entered the name when you created the service in the "To Create a Unified Messaging Service to Access Exchange from Cisco Unity Connection" procedure on page 2-37.

The display-only Service Type field should display "Exchange." If it displays another value, choose a different unified messaging service.

Step 6 In the Account Information section, select the applicable option for the Exchange mailbox that you want to access:

- **Use This Email Address**—If you want to specify an Exchange mailbox different from the one associated with the corporate email address, select this option, and enter the email address (the Active Directory primary SMTP address).
- **Use Corporate Email Address**—If you want to use the corporate email address, select this option. (You can edit the value in the Corporate Email Address field on the Edit User Basics page.)

Note If the unified messaging service that you selected in Step 5 specifies an Exchange server (instead of automatically searching for Exchange servers), and if users are using TTS to access email in Exchange 2003, you must also select an option in the Account Information (Used Only for Exchange 2003 TTS) section and, if applicable, specify a value for the User ID field.

Step 7 The Account Information (Used Only for Exchange 2003 TTS) section is applicable only when both of the following are true:

- Users are using TTS to access email in Exchange 2003.
- The unified messaging service that you selected in Step 5 specifies an Exchange server (instead of automatically searching for Exchange servers)

Select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the Active Directory domain alias for the user is the same as the Unity Connection user alias. Unity Connection signs into Exchange as the user by using the Unity Connection user alias.
- **Use User ID Provided Below**—Enter the Active Directory domain alias for the user. This option is useful when the User ID setting is different from the Unity Connection user alias. Unity Connection signs into Exchange as the user by using the setting in this field.

Step 8 Verify that the user has an SMTP proxy address that matches the email address that you specified in Step 6, either by entering a value for the Use This Email Address option or by choosing to use the corporate email address:

a. On the Edit menu, select **SMTP Proxy Address**.

b. If the SMTP Proxy Addresses page includes an entry for the email address that you specified in Step 6, skip to Step 9. Otherwise, continue with Step 8c.

c. Select **Add New**.

d. Add the email address that you specified in Step 6.

e. Select **Save**.

Step 9 The Service Capabilities section displays the options that are enabled in the unified messaging service that you selected in Step 5. If you want to disable any of the services for this user, uncheck the corresponding check box.

You can add more than one unified messaging service for a user, but the same service capability cannot be enabled in more than one unified messaging service for the same user. This also applies to Exchange calendars and MeetingPlace: you cannot configure a user to access Exchange calendars and MeetingPlace scheduling and joining.

For information on synchronization behavior if you later disable single inbox in a unified messaging account, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes" section on page 2-11.

Step 10 Select **Save**.

Step 11 To check the configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange, Active Directory, Cisco Unity Connection, and the Unity Connection user.

Step 12 Repeat Step 2 through Step 11 for all remaining users.

Testing Unified Messaging Accounts for Cisco Unity Connection

Do the following procedure to test one or more of the unified messaging accounts that you created in the "Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes" section on page 2-42.

To Test User Access to Exchange for Individual Cisco Unity Connection Users

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user who is configured for one or more unified messaging features for Exchange.

Note If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

Step 3 On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4 Select a unified messaging account for Exchange.

Step 5 On the Edit Unified Messaging Account page, select **Test**.

Step 6 Review the results, resolve problems, if any, and re-run the test until no more problems are found.

Viewing a Summary of the Configuration of Unified Messaging Accounts for Cisco Unity Connection

You can view a summary of the configuration for all of the unified messaging accounts on a Unity Connection server, including:

- Current status of Unity Connection configuration settings for each unified messaging account, which indicates whether consistency problems with Unity Connection settings prevent unified messaging from functioning correctly. When you select the status icon for a unified messaging account, the Unified Messaging Account page appears, and the status area of the page lists both problems and possible problems, if any.

You can also test whether a unified messaging account has connectivity with other servers by using the Test Connectivity button on the Unified Messaging Account page.

- The alias of the user associated with the account. When you select the alias for a unified messaging account, the Edit Unified Messaging Account page appears, and the status area of the page lists problems and possible problems, if any.
- The display name of the user associated with the unified messaging account.
- The name of the unified messaging service that is associated with the unified messaging account. When you select the service name, the Unified Messaging Services page appears with the settings for the service.
- The current unified messaging settings for each unified messaging account.

To View a Summary of the Configuration of Unified Messaging Accounts for Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging**, then select **Unified Messaging Account Status**.

Step 2 To sort by the values in a column in ascending order, select the heading for the column. To sort in descending order, select the heading again.

Step 3 To display the Unified Messaging Accounts page for an account, select the icon or the value of the Alias column in the applicable row.

Step 4 To display the Unified Messaging Services page for an account, select the value of the UM Services column in the applicable row.

Testing System Configuration, Including Unified Messaging, with Exchange and Cisco Unity Connection

You can run a Unity Connection system test that includes tests of the unified messaging configuration and that provides summary data on configuration problems, if any, for example, the number of accounts assigned to a specified unified messaging service that has configuration problems.

To Check System Configuration, Including Unified Messaging Configuration for Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Tools**, then select **Task Management**.

Step 2 On the Task Definitions page, select **Check System Configuration**.

Step 3 Select **Run Now**.

Step 4 Select **Refresh** to display links to the latest results.

Step 5 Review the results, resolve problems, if any, and re-run the Check System Configuration task until no more problems are found.

Testing Access to Exchange Calendars for Cisco Unity Connection

If you configured Unity Connection access to Exchange calendars, do the following procedure.

To Test Access to Exchange Calendars for Cisco Unity Connection

Step 1 Sign in to Outlook.

Step 2 On the Go menu, select **Calendar**.

Step 3 On the File menu, select **New > Meeting Request**.

Step 4 Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

Step 5 Select **Send**.

Step 6 Sign in to the Cisco Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

Step 7 If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Unity Connection reads the information about the Exchange meeting.

Resolving SMTP Domain Name Configuration Issues

Revised September, 2013

When a single inbox user receives a voice message, it is synchronized from Cisco Unity Connection to Microsoft Exchange. The email address of sender/recipient has Unity Connection domain name, for example, userid@CUC-hostname. Due to this, email clients like Microsoft Outlook or IBM Lotus Notes adds the Cisco Unity Connection address as "recent contacts" in the address book. When a user replies to an email or adds recipient while composing an email, the user can enter/select the Cisco Unity Connection address, which may lead to NDR. In case you desire when the voice message is synchronized for single inbox users from Connection to Exchange, the email address of sender/recipient is displayed as the corporate email address, for example, userid@corp-hostname, you must perform the following steps:

Step 1 In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Smart Host**.

Step 2 On the Smart Host page, in the Smart Host field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured).

Note Microsoft Exchange server can be used as a smart host.

Step 3 Click on Save.

Step 4 Configure SMTP Proxy addresses for users (For example, userid@corp-hostname). For more information see the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x chapter of *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Step 5 In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

Step 6 On the General Configuration page, in the **When a recipient cannot be found** list, select **Relay message to smart host** so that if the Recipient is not found, the message will be sent to the smart host.

Step 7 Click on Save.

Step 8 In Cisco Unity Connection Administration, expand **Users > Edit > Message Actions**. Select the Accept the message option from the Voicemail drop- down list. Make sure to select the Relay the message option from the Email, Fax, and receipt drop -down lists.

Step 9 Setup a recipient policy on Exchange Server such that the Cisco Unity Connection alias resolves to the corporate email Id.

- For Exchange 2013 or Exchange 2010, see the following link:

  http://technet.microsoft.com/en-us/library/bb232171.aspx
- For Exchange 2007, see the following link:
  http://technet.microsoft.com/en-us/library/bb232171(v=exchg.80).aspx
- For Exchange 2003, see the following link:

  http://support.microsoft.com/kb/822447
- For Configuring Exchange Email Policies with Unity Connection, please see the following white paper link:
  http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/ps12506/ps6509/guide_c07-728014.html.

CHAPTER 3

Configuring Cisco Unity Connection and Microsoft Office 365 for Unified Messaging

See the following sections:

About Unified Messaging with Office 365 in Cisco Unity Connection

See the following sections:

Accessing Office 365 Email by Using Text to Speech in Cisco Unity Connection

When Cisco Unity Connection is configured to allow access to Office 365 email by using text to speech, users have the option to hear their emails read to them when they sign in to Cisco Unity Connection by phone.

Accessing Office 365 Calendars and Contacts in Cisco Unity Connection

When Cisco Unity Connection is configured to access Office 365 calendars and contacts, Connection users can do the following by phone:

- Hear a list of upcoming meetings (Outlook meetings only).
- Hear a list of the participants for a meeting.
- Send a message to the meeting organizer.
- Send a message to the meeting participants.
- Accept or decline meeting invitations (Outlook meetings only).
- Cancel a meeting (meeting organizers only).

In addition, Connection enables users to import Office 365 contacts by using the Connection Messaging Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Connection Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

Synchronizing Voice Messages in Connection and Office 365 Mailboxes in Cisco Unity Connection (Single Inbox)

Revised September 13, 2013

If any unified users' Exchange mailboxes have more than 1000 messages, which includes voice messages and receipts, then enable the EWS paged view search functionality at Cisco Unity Connection. For more information on the paged view search functionality, see the "Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2013 and Later)" section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter of this guide.

This section describes how synchronizing voice messages in Connection and Office 365 mailboxes works. See the following sections:

- How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes, page 3-5
- How Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts Are Synchronized, page 3-6

Where Voice Messages Are Stored When Single Inbox Is Configured

All Connection voice messages, including those sent from Cisco Unity Connection ViewMail for Microsoft Outlook, are first stored in Connection and are immediately replicated to the Office 365 mailbox for the recipient.

How Single Inbox Works With ViewMail for Outlook

If you want users to use Outlook to send new Connection voice messages, or to reply to or forward voice messages, and if you want the messages to be synchronized with Connection:

- If you have not already done so, in Connection Administration, add SMTP proxy addresses for the Connection users that are configured for single inbox. The SMTP proxy address for a user must match the Office 365 email address that is specified in the unified messaging account in which single inbox is enabled.
- Install ViewMail for Outlook on user workstations. Without ViewMail for Outlook installed, voice messages are sent by Outlook as emails with .wav file attachments, and are treated as emails by Connection.
- On each user workstation, associate an email account with a Connection server.

Voice messages appear in the Outlook Inbox folder of the user, alongside other messages that are stored in Office 365; the voice messages also appear in the Connection mailbox of the user.

When single inbox is configured, Connection adds a Voice Outbox folder to the Outlook mailbox. Connection voice messages sent from Outlook do not appear in the Sent Items folder.

Private messages cannot be forwarded.

How Single Inbox Works without ViewMail for Outlook or with Other Email Clients

If you use another email client to access Connection voice messages in Office 365, or if you do not install ViewMail for Outlook:

- The email client treats Connection voice messages like emails with .wav file attachments.
- When a user replies to or forwards a Connection voice message, the reply or forward also is treated like an email, even if the user attaches a .wav file. Message routing is handled by Office 365, not by Connection, so the message is never sent to the Connection mailbox for the recipient.
- Users cannot listen to secure voice messages.
- It may be possible to forward private voice messages. (When users use ViewMail for Outlook, ViewMail for Outlook prevents private messages from being forwarded.)

Accessing Secure Voice Messages in the Exchange Mailbox

To play secure Connection voice messages in the Exchange mailbox, users must use Microsoft Outlook and Cisco Unity Connection ViewMail for Microsoft Outlook. Without ViewMail for Outlook installed, users accessing secure voice messages see only text in the body of a decoy message; the text briefly explains secure messages.

How Synchronization Works With Outlook Folders

Connection synchronizes voice messages in the following Outlook folders with the Connection Inbox folder for the user, so the messages are still visible in the Connection Inbox folder:

- Subfolders under the Outlook Inbox folder
- Subfolders under the Outlook Deleted Items folder
- The Outlook Junk Email folder

Messages in the Outlook Deleted Items folder appear in the Connection deleted items folder.

If the user moves voice messages (except secure voice messages) into Outlook folders that are not under the Inbox folder, the messages are moved to the deleted items folder in Connection. The messages can still be played by using ViewMail for Outlook because a copy still exists in the Outlook folder. If the user moves the messages back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Connection Inbox folder, and:

- If the message is still in the deleted items folder in Connection, the message is synchronized back into the Connection Inbox for that user.
- If the message is not still in the deleted items folder in Connection, the message is still playable in Outlook, but it is not resynchronized into Connection.

Secure voice messages behave differently. When Connection replicates a secure voice message to Office 365, it replicates only a decoy message that briefly explains secure messages; the only copy of the voice message remains on the Connection server. When a user plays a secure message by using ViewMail for Outlook, ViewMail retrieves the message from the Connection server and plays it without ever storing the message in Office 365 or on the computer of the user.

If the user moves a secure message to an Outlook folder that is not synchronized with the Connection Inbox folder, the only copy of the voice message is moved to the deleted items folder in Connection, and the message can no longer be played in Outlook. If the user moves the message back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Connection Inbox folder, and:

- If the message is still in the deleted items folder in Connection, the message is synchronized back into the Connection Inbox for that user, and the message becomes playable again in Outlook.
- If the message is not still in the deleted items folder in Connection, the message is not resynchronized into Connection and can no longer be played in Outlook.

Where Deleted Messages Go

By default, when a user deletes a voice message in Connection, the message is sent to the Connection deleted items folder and synchronized with the Outlook Deleted Items folder. When the message is deleted from the Connection deleted items folder (the user can do this manually, or you can configure message aging to do it automatically), it is also deleted from the Outlook Deleted Items folder.

If you are adding the single-inbox feature to an existing system, and if you have configured Connection to permanently delete messages without saving them in the deleted items folder, messages that users delete by using the Web Inbox or by using the Connection phone interface are still permanently deleted.

However, messages that users delete by using Outlook are only moved to the Deleted Items folder in Outlook, not permanently deleted. When Connection synchronizes with Office 365, the message is moved to the Connection deleted items folder; it is not permanently deleted. We recommend that you do one or both of the following:

- Configure message aging to permanently delete messages in the Connection deleted items folder.
- Configure message quotas, so that Connection prompts users to delete messages when their mailboxes approach a specified size.

When a user deletes a voice message from any Outlook folder, including the Outlook Inbox folder, the Deleted Items folder, or any subfolder, the message is moved to the deleted items folder in Connection. No operation in Outlook will cause a message to be permanently deleted in Connection.

Types of Connection Messages That Are Not Synchronized with Office 365

The following types of messages are not synchronized:

- Sent messages
- Draft messages
- Messages configured for future delivery but not yet delivered
- Broadcast messages
- Unaccepted dispatch messages. When a dispatch message has been accepted by a recipient, it becomes a normal message and is synchronized with Office 365 for the user who accepted it and deleted for all other recipients. Until someone on the distribution list accepts a dispatch message, the message waiting indicator for everyone on the distribution list will remain on, even when users have no other unread messages.

Replication of Status Changes

Status changes (for example, from unread to read), changes to the subject line, and changes to the priority are replicated from Connection to Exchange and vice versa, as applicable.

How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes

When you configure unified messaging, you create one or more unified messaging services that define, among other things, which unified messaging features are enabled. You also create one or more unified messaging accounts for each user to associate the user with unified messaging services. You can disable single inbox in three ways:

- Entirely disable a unified messaging service in which single inbox is enabled. This disables all enabled unified messaging features (including single inbox) for all users that are associated with the service.
- Disable only the single inbox feature for a unified messaging service, which disables only the single inbox feature for all users that are associated with that service.
- Disable single inbox for a unified messaging account, which disables single inbox only for the associated user.

If you disable and later re-enable single inbox by using any of these methods, Connection resynchronizes the Connection and Office 365 mailboxes for the affected users. Note the following:

- If users delete messages in Office 365 but do not delete the corresponding messages in Connection while single inbox is disabled, the messages will be resynchronized into the Office 365 mailbox when single inbox is re-enabled.
- If messages are hard deleted from Office 365 (deleted from the Deleted Items folder) before single inbox is disabled, the corresponding messages that are still in the deleted items folder in Connection when single inbox is re-enabled will be resynchronized into the Office 365 Deleted Items folder.
- If users delete messages in Connection but do not delete the corresponding messages in Office 365 while single inbox is disabled, the messages remain in Office 365 when single inbox is re-enabled. Users must delete the messages from Office 365 manually.
- If users change the status of messages in Office 365 (for example, from unread to read) while single inbox is disabled, the status of Office 365 messages will be changed to the current status of the corresponding Connection messages when single inbox is re-enabled.
- When you re-enable single inbox, depending on the number of users associated with the service and the size of their Connection and Office 365 mailboxes, resynchronization for existing messages may affect synchronization performance for new messages.

How Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts Are Synchronized

Connection can send heard/read receipts, delivery receipts, and non-delivery receipts to Connection users who send voice messages. If the sender of a voice message is configured for single inbox, the applicable receipt is sent to the Connection mailbox for the sender. The receipt is then synchronized into the Office 365 mailbox for the sender.

Note the following.

- *Read/heard receipts:* When sending a voice message, a sender can request a read/heard receipt. If you do not want Connection to respond to requests for read receipts, in Connection Administration, uncheck the Respond to Requests for Read Receipts check box, which appears on the Users > Users > Edit > Mailbox page and on the Templates > User Templates > Edit > Mailbox page.
- *Delivery receipts:* A sender can request a delivery receipt only when sending a voice message from ViewMail for Outlook. You cannot prevent Connection from responding to a request for a delivery receipt.
- *Non-delivery receipts (NDR):* A sender receives an NDR when a voice message cannot be delivered. If you do not want Connection to send an NDR when a message cannot be delivered, in Connection Administration, uncheck the Send Non-Delivery Receipts for Message Failed Delivery check box, which appears on the Users > Users > Edit User Basics page and on the Templates > User Templates > Edit User Template Basics page.

  Note the following about NDRs:

  - When the sender accesses Connection by using the TUI, the NDR includes the original voice message, which allows the sender to resend the message at a later time or to a different recipient.
  - When the sender accesses Connection by using Web Inbox, the NDR includes the original voice message, but the sender cannot resend it.
  - When the sender uses ViewMail for Outlook to access Connection voice messages that have been synchronized into Office 365, the NDR is a receipt that contains only an error code, not the original voice message, so the sender cannot resend the voice message.
  - When the sender is an outside caller, NDRs are sent to Connection users on the Undeliverable Messages distribution list. Verify that the Undeliverable Messages distribution list includes one or more users who regularly monitors and reroutes undelivered messages.

Task List for Configuring Cisco Unity Connection and Office 365 for Unified Messaging

To configure one or more unified messaging features, complete the following tasks in the order presented.

1. Review the "Requirements for Using Unified Messaging Features" section in the *System Requirements for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html .
2. *Cisco Unified Communications Manager Business Edition only:* Confirm that Connection is licensed for single inbox. See the "Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only)" section on page 3-10
3. *If Connection is integrated with an LDAP directory:* Review the current LDAP directory configurations to confirm that the Cisco Unified Communications Manager Mail ID field is synchronized with the LDAP mail field. During the integration process, this causes values in the LDAP mail field to appear in the Corporate Email Address field in Connection.

   Unified messaging requires that you enter the Office 365 email address for each Connection user. On the Unified Messaging Account page, each user can be configured to use either of the following values:

   - The Corporate Email Address specified on the User Basics page
   - The email address specified on the Unified Messaging Account page

   Email address field on the Unified Messaging Account page can be populated by using Connection Administration or the Bulk Administration Tool.

Note Connection supports on-premise LDAP directory integration only.

4. *If you are using single inbox and you want users to be able to use ViewMail for Outlook to send new voice messages, or to forward or reply to voice messages:* Install Cisco Unity Connection ViewMail for Microsoft Outlook on user workstations. For more information on installing ViewMail for Outlook, see the *Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook Release 8.5(x)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
5. Synchronization threads configuration should be done based on latency between Connection and Office 365 server. For more information, refer to "Latency" section of the design guide at

   http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/design/guide/8xcucdg032.html.
6. Decide whether you want Connection to be able to search for and communicate with different Office 365 server, or you want Connection to communicate with a specific Office 365 server in case the hostname or the IP Address of the specific Office 365 server is known**. Auto Discovery is the recommended option**.

   If Connection is not already configured to use DNS, use the following CLI commands to configure DNS:

   - set network dns
   - set network dns options

   We recommend that you configure Connection to use the same DNS environment in which the Active Directory environment is publishing its records.

For more information on the CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

7. Create an Active Directory account to be used for Connection unified messaging services, and grant the account the applicable permissions. See the "Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection" section on page 3-10.
8. If you are using single inbox and users do not already have added SMTP proxy addresses: Add proxy addresses to Connection user accounts. For more information, see the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.
9. Update class of service settings as required:
   - Enable single inbox in one or more classes of service. For more information, see the "Single Inbox in Cisco Unity Connection" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

     Note that all users who are configured to use single inbox must be in a class of service in which single inbox is enabled.

     Cisco Unified Communications Manager Business Edition only: Connection counts all users in a class of service in which single inbox is enabled as single inbox users even if they are not configured to use single inbox. For example, if a Connection server is licensed for 200 single-inbox users, and if you have three classes of service in which single inbox is enabled, the total number of users assigned to those three classes of service cannot exceed 200 users. This is true even if you only configure 50 users to use single inbox.
   - Enable text-to-speech access to Exchange voice messages on one or more classes of service: check the Allow Access to Advanced Features check box on the applicable class of service page, and then check the Allow Access to Exchange Email by Using Text to Speech (TTS) check box.
10. *If classes of service for single-inbox users have Delete Messages Without Saving to Deleted Items Folder enabled:* We recommend that you configure message aging and/or message quotas. Otherwise, messages deleted from Outlook may never be permanently deleted from Connection. For more information, see the "Synchronizing Voice Messages in Connection and Office 365 Mailboxes in Cisco Unity Connection (Single Inbox)" section on page 3-2.

    For more information on configuring message aging and message quotas for Connection, see the "Controlling the Size of Mailboxes in Cisco Unity Connection 9.x" chapter in the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
11. Configure one or more Connection unified messaging services. See the "Creating a Unified Messaging Service to Access Office 365 from Cisco Unity Connection" section on page 3-12.
12. *Selected configurations:* For the following configuration, upload SSL certificates on the Connection server to encrypt communication between Connection and Office 365 and between Connection and Active Directory:

- If you configured Connection to search for and communicate with different Exchange servers, to use LDAPS to communicate with domain controllers, and to validate certificates for domain controllers in Task 10.

Caution When you allow Connection to search for and communicate with Office 365 servers, Connection communicates with Active Directory servers using Basic authentication. By default, the user name and password of the unified messaging services account and all other communication between the Connection and Active Directory servers is sent in clear text. If you want this data to be encrypted, in Task 11. you must configure unified messaging services to communicate with Active Directory domain controllers by using the secure LDAP (LDAPS) protocol.

For more information, see the Uploading CA Public Certificates for Exchange and Active Directory Servers to the Cisco Unity Connection Server, page 2-40.

13. Test the unified messaging configuration. See the following sections:
    - Testing Unified Messaging Services for Cisco Unity Connection, page 3-14
    - Testing Unified Messaging Accounts for Cisco Unity Connection, page 3-15
    - Testing System Configuration, Including Unified Messaging, with Office 365 and Cisco Unity Connection, page 3-15
    - Testing Access to Office 365 Calendars for Cisco Unity Connection, page 3-16
14. *If Connection voice messages are automatically being moved to the Outlook Junk Items folder:* Change the Outlook configuration to add the sender of the voice message or the sender's domain to the safe sender's list. For more information, see Outlook Help.
15. To teach users how to use the Connection calendar, refer them to the following:
    - For listing, joining, and scheduling meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucugphone.html.
    - For importing Exchange contacts, see the "Managing Your Personal Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcucugasst.html.
    - For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/pctr/b_9xcucugpctr.html.

Note Office 365 servers, which Connection accesses have authentication mode set to Basic and web-based protocol set to HTTPS.

Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection

Cisco Unity Connection accesses Office 365 mailboxes by using a domain service account called the unified messaging services account. After you create the account, you grant it the rights necessary for Connection to perform operations on behalf of the user.

See the following section:

Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection, page 3-10

Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection

1. Create one or more service accounts on the Office 365 servers with which you want Connection to communicate. Note the following:
   - Give the account a name that identifies it as the unified messaging services account for Connection.
   - Do not add the account to any administrator group.
   - Do not disable the account, or Connection cannot use it to access Office 365 mailboxes.
   - Specify a password that satisfies the password-security requirements of your company. The password is encrypted with AES 128-bit encryption and stored in the Connection database. The key that is used to encrypt the password is accessible only with root access, and root access is available only with assistance from Cisco TAC.
   - When you are configuring unified messaging for a Connection cluster, Connection automatically uses the same unified messaging services account for both Connection servers.
   - When you are configuring unified messaging for intersite networking or for intrasite networking, you can use the same unified messaging services account for more than one Connection server. However, this is not a requirement and does not affect functionality or performance.
2. For Assigning the Impersonation Rights to Service Accounts see the following Section,*Release 9.x* at Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only), page 3-10

Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only)

Revised June 3, 2013

To Assign the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 Only)

Step 1 To configure impersonation in Office 365, you must run a Windows PowerShell script. For details see the, "Accessing Office 365 Using Remote Exchange Management PowerShell" section on page 3-11 section.

Step 2 You must have the permission to run the **New-ManagementRoleAssignment** cmdlet. By default the administrators have this permission.

Use "**New-ManagementRoleAssignment**" Exchange Management Shell cmdlet to grant the service account permission to impersonate all the users in the organization.

new-ManagementRoleAssignment -Name:RoleName -Role:ApplicationImpersonation -User:Account

where:

–Name parameter specifies the name of the new role assignment, for example, ConnectionUMServicesAcct. The name that you enter for RoleName appears when you run get-ManagementRoleAssignment.

-Role parameter indicates that the ApplicationImpersonation role is assigned to the user specified by the User parameter.

–User is the name of the unified messaging services account in alias@domain format.

For example:

New-ManagementRoleAssignment –Name "ConnectionUMServicesAcct" –Role "ApplicationImpersonation" –User serviceaccount@example.onmicrosoft.com

Note This operation may not be allowed for the organization with the disabled customizations. In order to enable this operation, you need to execute the Enable-OrganizationCustomization task first, that is "*Enable-OrganizationCustomization*".

Step 3 If you created more than one unified messaging services account, repeat Step 2 for the remaining accounts. Specify a different value for RoleName for each unified messaging services account.

Caution If you have activated the Active Directory Synchronization feature and migrating from local Exchange server to Office 365, then the further user management is done through the on-premises Active Directory Services and it gets synchronized with Office 365 automatically. You must make sure the Application Impersonation Management role is given to your Office 365 server.

Accessing Office 365 Using Remote Exchange Management PowerShell

Revised October 23, 2013

To Access Office 365 Using Remote Exchange Management Power Shell

Step 1 Run Windows PowerShell as administrator and run following Command.

Set-ExecutionPolicy Unrestricted

Step 2 On a Windows PowerShell endpoint, run the following command and enter the Office-365 administrator account credentials for authentication in the popup window.

$LiveCred = Get-Credential

Step 3 To establish a remote Windows PowerShell session with Office 365, use the New-PSSession Windows PowerShell cmdlet to connect with the generic remote Windows PowerShell endpoint at http://ps.outlook.com/powershell. Run the following command to create Remote Exchange Shell Session.

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection

Note The user account you use to connect to office 365 Exchange Online must be enabled for remote shell.

Step 4 Run the following command to Import all Remote Exchange Shell Commands to the local client side session.

Import-PSSession $Session

If it fails with an error message we may need to set the Execution policy to allow running remote PowerShell scripts.Run Get-ExecutionPolicy. If the value returned is anything other than RemoteSigned, you need to change the value to RemoteSigned by running Set-ExecutionPolicy RemoteSigned

http://technet.microsoft.com/en-us/library/jj984289%28v=exchg.150%29.aspx

To use Import-PSSession, the execution policy in the current session cannot be Restricted or All signed, because the temporary module that Import-PSSession creates contains unsigned script files that are prohibited by these policies. To use Import-PSSession without changing the execution policy for the local computer, use the Scope parameter of Set-ExecutionPolicy to set a less restrictive execution policy for a single process.

http://community.office365.com/en-us/forums/158/t/71614.aspx

Creating a Unified Messaging Service to Access Office 365 from Cisco Unity Connection

Revised June 3, 2013

Do the following procedure to create one or more unified messaging services.

To Create a Unified Messaging Service to Access Office 365 from Cisco Unity Connection 8.6(2) and Later

Step 1 In Cisco Unity Connection Administration, expand Unified Messaging, then select Unified Messaging Services.

Step 2 On the Search Unified Messaging Services page, select **Add New**.

Step 3 Decide which options to select for the Message Action for Email and Message Action for Fax lists at the bottom of the page. (For field information, on the Help menu, select This Page.)

If you want to select Relay the Message or Accept and Relay the Message for either list, you must first configure an SMTP Smart Host on the System Settings > SMTP Configuration > Smart Host page. Connection Administration will not let you save a new unified messaging configuration with those settings when no SMTP Smart Host is configured. For SMTP smart host server, Connection will communicate with on -premise SMTP relay servers only.

Step 4 On the New Unified Messaging Service page, in the Type list, select **Office 365**.

Note You can configure up to 1800 users with a single Office 365 Unified Messaging Service. For creating more than 1800 users with Office 365, you need to create more Unified Messaging services.

Step 5 Check the **Enabled** check box to enable the service.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes" section on page 3-5

Step 6 In the **Display Name** field, enter a descriptive name.

If you are creating more than one unified messaging service for Office 365, note that this is the name that will appear on the **Users > Unified Messaging Accounts page** when you configure users for unified messaging. Enter a display name that will simplify choosing the correct unified messaging service for each user.

Step 7 If you want Connection to validate the SSL certificate from the Exchange server, check the Validate Certificates for Exchange Servers check box.

Step 8 In the **Proxy Server** field, enter the IP Address and port in the Adress:Port or Hostname:Port format.

Note Proxy Server is an optional field that allows you to route the traffic using a Proxy server when the Office 365 network is not accessible from Connection.

Step 9 If you want Connection to automatically find Hosted Exchange client access servers, do the following:

a. Select **Search for Hosted Exchange Servers**.

Note It is mandatory to use Search for Hosted Exchange Servers option with Office 365.

b. Enter DNS Domain Name used for the Office 365 users.

- In a hybrid environment where you route mails between an on-premise Exchange organization and Office 365, specify the special onmicrosoft.com domain name (such as mycompany.mail.onmicrosoft.com) provided by Microsoft.
- If you are only using Office 365, try your domain name from your email addresses.

c. If you have Hosted Exchange servers in more than one Active Directory site, you can improve performance if you specify the site that contains the domain controllers that you want Connection to use to find Exchange servers. In the Active Directory Site Name field, enter the name of the site.

d. In the **Protocol Used to Communicate with Domain Controllers** list, select whether Connection should use LDAP or secure LDAP (LDAPS) when communicating with Active Directory to find Hosted Exchange servers.

Caution Caution: When you select Search for Hosted Exchange Servers, Connection communicates with Active Directory servers using Basic authentication. As a result, the username and password of the unified messaging services account and all other communication between the Connection and Active Directory servers is in clear text. If you want this data to be encrypted, you must select Secure LDAP (LDAPS) in the Protocol Used to Communicate with Domain Controllers list and upload certificates from the certification authority that issued the SSL certificates for Active Directory servers to both tomcat-trust and Connection-trust locations.

e. If you want Connection to validate the SSL certificate from Active Directory domain controllers, check the **Validate Certificates for Active Directory Domain Controllers** check box.

   Self-signed certificates cannot be validated. If you selected LDAPS from the **Protocol Used to Communicate with Domain Controllers list**, and if you are using self-signed certificates, do not check the Validate Certificates for **Active Directory Domain Controllers** check box. If you do check the check box, Connection will not be able to access domain controllers to search for Hosted Exchange servers.

f. Skip to Step 9.

Step 10 In the Username and Password fields, enter the Active Directory username and password for the Domain Service account provided by Microsoft Office 365.

The username must be in User Principal Name(username@domain.com) format.

Step 11 Under Service Capabilities, select the features that you want this unified messaging service to allow.

Note When you configure unified messaging for Connection users, you can disable for an individual user any feature that you enable here. However, you cannot enable for an individual user any feature that you disable here.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes" section on page 3-5

Step 12 Under Synchronize Connection and Office 365 Mailboxes (Single Inbox), choose message actions for email and for fax. (For field information, on the Help menu, select This Page.)

Step 13 Select **Save**

Testing Unified Messaging Services for Cisco Unity Connection

Do the following procedure to test one or more unified messaging services.

To Test Unified Messaging Services for Connection

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging**, then select **Unified Messaging Services**.

Step 2 On the Search Unified Messaging Services page, select the service that you want to test.

Step 3 On the Edit Unified Messaging Service page, select **Test**.

Step 4 If the test results showed configuration problems, resolve the problems, then repeat the test.

Step 5 If you configured two or more unified messaging services, repeat Step 1 through Step 4 to test the remaining services.

Testing Unified Messaging Accounts for Cisco Unity Connection

Do the following procedure to test one or more of the unified messaging accounts that you created in the Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection, page 3-10

To Test User Access to Office 365 for Individual Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user who is configured for one or more unified messaging features for Office 365.

Note If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

Step 3 On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4 Select a unified messaging account for Exchange.

Step 5 On the Edit Unified Messaging Account page, select **Test**.

Step 6 Review the results, resolve problems, if any, and re-run the test until no more problems are found.

Testing System Configuration, Including Unified Messaging, with Office 365 and Cisco Unity Connection

You can run a Connection system test that includes tests of the unified messaging configuration and that provides summary data on configuration problems, if any, for example, the number of accounts assigned to a specified unified messaging service that has configuration problems.

To Check System Configuration, Including Unified Messaging Configuration for Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Tools**, then select **Task Management**.

Step 2 On the Task Definitions page, select **Check System Configuration**.

Step 3 Select **Run Now**.

Step 4 Select **Refresh** to display links to the latest results.

Step 5 Review the results, resolve problems, if any, and re-run the Check System Configuration task until no more problems are found.

Testing Access to Office 365 Calendars for Cisco Unity Connection

If you configured Connection access to Office 365 calendars, do the following procedure.

To Test Access to Office 365 Calendars for Cisco Unity Connection

Step 1 Sign in to Outlook.

Step 2 On the Go menu, select **Calendar**.

Step 3 On the File menu, select **New > Meeting Request**.

Step 4 Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

Step 5 Select **Send**.

Step 6 Sign in to the Cisco Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

Step 7 If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Connection reads the information about the Exchange meeting.

CHAPTER 4

Moving Microsoft Exchange Mailboxes for Connection Users Who Are Configured for Unified Messaging

See the following sections:

Determining When You Must Update Cisco Unity Connection User Settings Manually After You Move Exchange Mailboxes

Revised May 29, 2013

If you create one or more unified messaging services for Exchange, as described in the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter, one of the settings identifies the Exchange servers that Connection communicates with:

- If you choose to allow Connection to search for Exchange servers, Connection can automatically detect when you move mailboxes from one version of Exchange to another and can automatically update Connection user settings.
- If you choose a specific Exchange server, Connection can sometimes detect when you move mailboxes from one Exchange server to another, and can automatically update hidden Connection user settings. When Connection cannot detect mailbox moves, you must manually replace the unified messaging account that accesses the old Exchange server with a unified messaging account that accesses the new server. Table 4-1 identifies when Connection can and cannot automatically detect mailbox moves between Exchange servers.

Table 4-1 When Connection Can Detect Mailbox Moves Between Exchange servers

If you choose a specific	Connection can automatically detect mailbox moves between the following Exchange versions								
	2003 and 2003	2003 and 2007	2003 and 2010	2007 and 2007	2007 and 2010	2010 and 2010	2007 and 2013	2010 and 2013	2013 and 2013
Exchange 2003 server	No	No	No	No	No	No	No	No	No
Exchange 2007 server	No	No	No	Yes	No	No	No	No	No
Exchange 2010 server	No	No	No	Yes	Yes	Yes	No	No	No
Exchange 2013 server	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

If Connection cannot automatically detect mailbox moves, do the procedure in the "Replacing Connection Unified Messaging Accounts After You Move Exchange Mailboxes" section on page 4-2.

Moving Exchange Mailboxes to a New Exchange Server for Connection

If you add an Exchange server to the Exchange organization, you want to move Exchange mailboxes to the new server, and the Exchange mailboxes are associated with Connection users who are configured for single inbox, you must grant the permissions that Connection requires before you move the mailboxes. Otherwise, Connection users will not be able to access their voice messages in the new location. This is true regardless of whether you allow Connection to search for Exchange servers or you configure Connection to communicate with a specific Exchange server.

For information on granting the necessary permissions, see the "Creating the Unified Messaging Services Account in Active Directory and Granting Permissions for Cisco Unity Connection" section on page 2-28. Note that creating a new unified messaging services account for the new Exchange server is not necessary; you can also grant an existing unified messaging services account the permissions required to access the new Exchange server.

Replacing Connection Unified Messaging Accounts After You Move Exchange Mailboxes

When Connection cannot detect Exchange mailbox moves and, therefore, cannot automatically update the location of the Exchange mailbox for a Connection user, you must manually create a new unified messaging account that accesses the new mailbox location and delete the unified messaging account that accessed the old mailbox location.

Caution Between the time that you move Exchange mailboxes and the time that you update Connection settings for the affected users, Connection will not synchronize voice messages with the corresponding Exchange mailboxes.

To Replace Connection Unified Messaging Accounts After You Move Exchange Mailboxes

Step 1 Review the "Determining When You Must Update Cisco Unity Connection User Settings Manually After You Move Exchange Mailboxes" section on page 4-1 to determine whether Connection can automatically detect mailbox moves for your Exchange configuration and Connection settings:

- If Connection can detect mailbox moves, skip the rest of this procedure.
- If Connection cannot detect mailbox moves, continue with Step 2.

Step 2 If you moved the Exchange mailbox to an Exchange server for which there is currently no Connection unified messaging service, create the service. For more information, see the "Creating a Unified Messaging Service to Access Exchange from Cisco Unity Connection" section on page 2-37.

Step 3 Create a new unified messaging account for the user, and choose a unified messaging service that accesses the Exchange server to which the mailbox was moved. For more information, see the "Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Exchange Mailboxes" section on page 2-42.

Step 4 Delete the unified messaging account that accessed the Exchange server from which the mailbox was moved:

a. In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

b. On the Search Users page, select the alias of a user.

Note If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

c. On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

d. On the Unified Messaging Accounts page, check the check box to the left of the unified messaging account that you want to delete.

e. Select **Delete Selected**.

Step 5 Repeat Step 2 through Step 4 for the other Connection users whose Exchange mailboxes you moved.

CHAPTER 5

Restoring Microsoft Exchange Mailboxes in Cisco Unity Connection When Single Inbox Is Enabled

This chapter contains the following sections:

Why Disabling Single Inbox Is Important Before Restoring Exchange Mailboxes for Cisco Unity Connection

If you want to restore Exchange mailboxes and the single-inbox unified messaging service capability is enabled for Cisco Unity Connection users whose Exchange mailboxes are being restored, you must disable single inbox for those users before you restore Exchange.

For information on how disabling single inbox affects synchronization behavior, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes" section on page 2-11.

Caution If you do not disable single inbox for Connection users whose Exchange mailboxes are being restored, Connection will not resynchronize voice messages that were received between the time that the backup from which you are restoring was created and the time that the restore is complete.

Connection maintains a synchronization cache that tracks which voice messages have already been forwarded to Exchange. When you disable single inbox, the synchronization cache is automatically cleared. Here is how it works:

1. You back up Exchange.
2. A new voice message arrives.
3. Connection synchronizes the voice message with the Exchange mailbox associated with the Connection user.

4. Connection updates the synchronization cache for that user to indicate that the message has been synchronized with Exchange.
5. A hard disk in the Exchange server fails.
6. You disable single inbox for the Connection user whose Exchange mailbox was on the failed hard disk.
7. Connection clears the synchronization cache for that user.
8. You replace the hard disk and restore Exchange from the backup that you made in 1.
9. You re-enable single inbox for the user.
10. Connection performs a periodic comparison of the synchronization cache with the voice messages currently in Exchange.
11. Because the cache is empty, Connection concludes that voice messages that are in the Connection mailbox but not in the Exchange mailbox have not yet been synchronized with Exchange.
12. Connection resynchronizes the Connection mailbox with the Exchange mailbox, and rebuilds the synchronization cache.

If you restore Exchange mailboxes without disabling single inbox for the Connection users, here is an explanation of why Connection deletes all voice messages that were received after the backup from which you are restoring:

1. You back up Exchange.
2. A new voice message arrives.
3. Connection synchronizes the voice message with the Exchange mailbox associated with the Connection user.
4. Connection updates the synchronization cache for that user to indicate that the message has been synchronized with Exchange.
5. A hard disk in the Exchange server fails.
6. You replace the hard disk and restore Exchange from the backup that you made in 1.
7. Connection performs a periodic comparison of the synchronization cache with the voice messages currently in Exchange. The voice message that arrived in 2. is not in the Exchange mailbox for the associated Connection user.
8. Connection concludes that the voice message has already been synchronized with Exchange and does not resynchronize the message into the Exchange mailbox.

Task List for Restoring Microsoft Exchange Mailboxes in Cisco Unity Connection When Single Inbox Is Enabled

1. Disable single inbox for selected users or for a unified messaging service. See the "Disabling Single Inbox for Cisco Unity Connection" section on page 5-3.
2. Restore Exchange mailboxes. For more information, see the applicable Microsoft documentation.
3. Re-enable single inbox by reversing the procedure that you used to disable single inbox in Task 1.:
   - If you disabled single inbox for individual users by using Connection Administration, repeat the "To Disable Single Inbox for Individual Users for Connection" procedure on page 5-4, but check the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box.

- If you disabled single inbox for a unified messaging service, repeat the "To Disable Single Inbox for All of the Users Associated with a Unified Messaging Service for Connection" procedure on page 5-4, but check either the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box or the **Enabled** check box, as applicable.
- If you disabled single inbox for individual users by using the Bulk Administration Tool, repeat the "To Disable Single Inbox for a Large Numbers of Selected Users by Using the Bulk Administration Tool for Connection" procedure on page 5-5, but change the value of enableMbxSynch to **1**.

Disabling Single Inbox for Cisco Unity Connection

The first step in restoring Exchange mailboxes is to disable single inbox, as noted in the "Why Disabling Single Inbox Is Important Before Restoring Exchange Mailboxes for Cisco Unity Connection" section on page 5-1. You can do so in several ways, depending on how many Exchange mailboxes you are restoring, whether you are restoring Exchange mailboxes for all of the associated with a unified messaging service, and how concerned you are about affecting Connection functionality during the restore.

Note For information on how disabling single inbox affects synchronization, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange Mailboxes" section on page 2-11.

Restoring Exchange Mailboxes for a Small Number of Users

If you are restoring Exchange mailboxes for a small number of users, you can disable single inbox on individual user accounts by using Connection Administration. See the "To Disable Single Inbox for Individual Users for Connection" procedure on page 5-4.

Restoring Exchange Mailboxes for All of the Users Associated with a Unified Messaging Service, or Restoring Mailboxes When Connection Functionality Is Not a Concern

When you are restoring Exchange mailboxes and either of the following is true, you can disable single inbox for a unified messaging service, which disables single inbox functionality for all users associated with the unified messaging service:

- You are restoring mailboxes for all of the users associated with a unified messaging service.
- You are restoring mailboxes for selected users associated with a unified messaging service, and you are restoring mailboxes during non-business hours, when interrupting single inbox functionality has less impact on users.

There are two ways to disable single inbox for a unified messaging service:

- *Disable only single inbox for a unified messaging service:* If you disable only single inbox, the Connection conversation continues to play the options for the other unified messaging features. If a user selects one of these features while Exchange is unavailable, the Connection conversation announces that access to messages is unavailable at this time.
- *Disable an entire unified messaging service:* If the unified messaging service also has the other unified messaging features enabled and you disable the service, the Connection conversation stops playing the options for those features until the unified messaging service is re-enabled, which could be confusing for users.

See the "To Disable Single Inbox for All of the Users Associated with a Unified Messaging Service for Connection" procedure on page 5-4.

Restoring Exchange Mailboxes for Some but Not All Users Associated with a Unified Messaging Service When Connection Functionality Is a Concern

When you are restoring Exchange mailboxes for a large number of users who are associated with a unified messaging service and both of the following are true, you can use the Bulk Administration Tool to disable single inbox for individual users:

- The unified messaging service also includes users whose mailboxes you are not restoring.
- You are restoring the mailboxes during business hours, when you want to minimize the impact on users whose mailboxes you are not restoring.

See the "To Disable Single Inbox for a Large Numbers of Selected Users by Using the Bulk Administration Tool for Connection" procedure on page 5-5.

To Disable Single Inbox for Individual Users for Connection

Step 1 In Connection Administration, select **Users**.

Step 2 On the Search Users page, select the alias of the user account that you want to modify.

Note If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

Step 3 On the Edit menu, select **Unified Messaging Accounts**.

Step 4 Select the unified messaging account that enables single inbox for this user.

Step 5 Uncheck the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box.

Step 6 Select **Save**.

Step 7 Repeat Step 1 through Step Step 6 for the remaining users.

To Disable Single Inbox for All of the Users Associated with a Unified Messaging Service for Connection

Step 1 In Connection Administration, select **Unified Messaging > Unified Messaging Services**.

Step 2 On the Search Unified Messaging Services page, select the alias of the unified messaging service that you want to modify.

Note If the unified messaging service does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

Step 3 To disable only single inbox for the users associated with this unified messaging service, uncheck the **Synchronize Connection and Exchange Mailboxes (Single Inbox)** check box.

To disable the entire unified messaging service, uncheck the **Enabled** check box.

Step 4 Select **Save**.

Step 5 Repeat Step 1 through Step 4 for other unified messaging services for which you want to disable single inbox.

To Disable Single Inbox for a Large Numbers of Selected Users by Using the Bulk Administration Tool for Connection

Step 1 In Connection Administration, select **Tools > Bulk Administration Tool**.

Step 2 Under Select Operation, select **Export**.

Step 3 Under Select Object Type, select **Unified Messaging Accounts**.

Step 4 Specify a filename for the CSV file to which unified messaging accounts are exported.

Step 5 Select **Submit**.

Step 6 Follow the onscreen prompts to save the CSV file.

Step 7 Open the CSV file.

Step 8 For the users for whom you want to disable the single-inbox feature, change the value of enableMbxSynch to **0**.

Step 9 In Connection Administration, select **Tools > Bulk Administration Tool**.

Step 10 Under Select Operation, select **Update**.

Step 11 Under Select Object Type, select **Unified Messaging Accounts**.

Step 12 Specify the name of the CSV file that you updated in Step 8.

Step 13 Select **Submit**.

CHAPTER 6

Configuring Cisco Unity Connection and Cisco Unified MeetingPlace for Unified Messaging

When integrated with Cisco Unified MeetingPlace 9.x, Cisco Unity Connection enables users to do the following by phone:

- Join a meeting that is in progress.
- Hear a list of the participants for a meeting.
- Send a message to the meeting organizer.
- Send a message to the meeting participants.
- Set up immediate meetings.
- Cancel a meeting (meeting organizers only).

See the following sections:

Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace

Use the following task list to create a calendar integration with Cisco Unified MeetingPlace:

1. Review the system requirements to confirm that all requirements for Cisco Unified MeetingPlace and the Cisco Unity Connection server have been met. See the "Requirements for the Cisco Unified MeetingPlace Calendar Integration" section on page 6-2.
2. Configure Cisco Unified MeetingPlace. See the "Configuring Cisco Unified MeetingPlace for the Calendar Integration" section on page 6-2.

3. Configure Connection. See the "Creating a Unified Messaging Service to Access Cisco Unified MeetingPlace from Cisco Unity Connection" section on page 6-4.
4. If you configured Cisco Unified MeetingPlace to use HTTPS in Task 2., and configured unified messaging services to validate certificates for MeetingPlace servers in Task 3.: on the Connection server, in Cisco Unified Communications Operating System, upload certificates from the certification authority that issued the SSL certificates for MeetingPlace servers to both tomcat-trust and Connection-trust locations.

   For SSL instructions, see the "Using SSL to Secure Client/Server Connections in Cisco Unity Connection 9.x" chapter of the *Security Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.
5. Configure the Connection users. See the "Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Cisco Unified MeetingPlace Users" section on page 6-5.
6. Test the calendar integration. See the "Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration" section on page 6-6.
7. To teach users how to list, join, and schedule meetings, see the "Managing Meetings" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucugphone.html.

Requirements for the Cisco Unified MeetingPlace Calendar Integration

The calendar integration with Cisco Unified MeetingPlace has the following requirements:

- Cisco Unified MeetingPlace 9.x as described in the "Requirements for Accessing Calendar Information for Meetings" section of *System Requirements for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/installation/guide/9xcucigx.html.

Configuring Cisco Unified MeetingPlace for the Calendar Integration

Do the following procedures:

- To Configure Cisco Unified MeetingPlace for the Calendar Integration, page 6-2
- To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration, page 6-3

To Configure Cisco Unified MeetingPlace for the Calendar Integration

Step 1 Sign in to the Cisco Unified MeetingPlace Application Server as an administrator.

Step 2 Select **User Configuration > User Profiles**.

Step 3 Select **Add New**.

Step 4 Enter the following values in the required fields to create a privileged service account:

First Name	Leave this field blank.
Last Name	Enter **Cisco Unity Connection**.
User ID	Enter **cucsvc** or another user ID that you want.
User Password	Enter the applicable password.
Profile Number	Enter the applicable profile number.
Profile Password	Enter the applicable profile password.
Type of User	Select **System Administrator**.

Note The values that you enter for the User ID, User Password, Profile Number, and Profile Password fields will be used in the "Creating a Unified Messaging Service to Access Cisco Unified MeetingPlace from Cisco Unity Connection" section on page 6-4.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace.

Caution If you do not sign out of Cisco Unified MeetingPlace, the test will fail in the "To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration" procedure on page 6-3.

To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration

Step 1 In the Address field of a web browser, if SSL is not enabled, enter the following URL (where <server> is the IP address or host name of the Cisco Unified MeetingPlace server):

http://<server>/webservices/services/meetingservice?wsdl

If SSL is enabled, enter the following URL:

https://<server>/webservices/services/meetingservice?wsdl

Step 2 Press **Enter**.

Step 3 When prompted to sign in, enter the user ID and password for the privileged service account that you created in the "To Configure Cisco Unified MeetingPlace for the Calendar Integration" procedure on page 6-2.

The Cisco Unified MeetingPlace WSDL download page appears with the title "XFire Services."

Creating a Unified Messaging Service to Access Cisco Unified MeetingPlace from Cisco Unity Connection

Do the following procedure.

To Create a Unified Messaging Service to Access Cisco Unified MeetingPlace from Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, select **Unified Messaging > Unified Messaging Services**.

Step 2 On the Search Unified Messaging Services page, select **Add New**.

Step 3 On the New Unified Messaging Service page, in the Type list, select **MeetingPlace 9.x**.

Step 4 Check the **Enabled** check box to enable the service.

When this check box is not checked, the integration with Cisco Unified MeetingPlace is disabled.

Step 5 In the Display Name field, enter a descriptive name.

Step 6 In the Server field, enter the IP address or host name for the Cisco Unified MeetingPlace server.

Step 7 In the Transfer Extension Dial String field, enter the digits that Connection must dial to transfer users on the phone to the opening greeting of Cisco Unified MeetingPlace server.

Step 8 In the Web-Based Protocol field, select **HTTPS** or **HTTP**, as applicable.

If you selected HTTPS and you want Connection to validate the Cisco Unified MeetingPlace server certificate, check the **Validate Certificates for MeetingPlace Servers** check box.

Caution The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of Server field. Otherwise, validation of the server certificate will fail.

The root certificate or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate must be installed as Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

Step 9 In the User ID field, enter the user ID for the privileged service account that Connection uses to sign in to the Cisco Unified MeetingPlace server.

This setting must match the User ID setting for the privileged service account that you configured in the "Configuring Cisco Unified MeetingPlace for the Calendar Integration" section on page 6-2.

Step 10 In the Password field, enter the password for the privileged service account that Connection uses to sign in to the Cisco Unified MeetingPlace server.

This setting must match the User Password setting for the privileged service account that you configured in the "Configuring Cisco Unified MeetingPlace for the Calendar Integration" section on page 6-2.

Step 11 Under Service Capabilities, check the applicable check boxes:

- **Announce MeetingPlace Meetings**—Check this check box so that users can hear of their upcoming meetings by phone.
- **MeetingPlace Scheduling and Joining**—Check this check box so that users can schedule and join meetings.

Step 12 Select **Save**.

Step 13 To check the integration with Cisco Unified MeetingPlace, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace and Cisco Unity Connection.

Creating Unified Messaging Accounts to Link Cisco Unity Connection Users to Cisco Unified MeetingPlace Users

Do the following procedure.

Caution Cisco Unified MeetingPlace must have an end user for each Connection user that you are configuring.

To Create Unified Messaging Accounts to Link Cisco Unity Connection Users to Cisco Unified MeetingPlace Users

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user.

Step 3 On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4 On the Unified Messaging Accounts page, select **Add New**. The New Unified Messaging Account page appears.

Step 5 In the Unified Messaging Service field, select the display name that you entered in the "Creating a Unified Messaging Service to Access Cisco Unified MeetingPlace from Cisco Unity Connection" section on page 6-4.

Step 6 In the Sign-In Type field, select the applicable option:

- **Use Connection Alias**—This option is useful when the Cisco Unified MeetingPlace profile alias is the same as the Connection user alias. Connection signs in the user with the Connection user alias. Cisco Unified MeetingPlace provides information on public and private meetings to the user.
- **Use Server Guest Account**—Connection signs in the user as a guest, without using the Connection user alias or the User ID setting. Cisco Unified MeetingPlace provides information only on public meetings to the user.
- **Use User ID Provided Below**—Enter the profile alias from Cisco Unified MeetingPlace (useful when the Cisco Unified MeetingPlace profile alias is different from the Connection user alias). Connection signs in the user with the setting in this field. Cisco Unified MeetingPlace provides information on public and private meetings to the user.

Step 7 *(Only when the Use User ID Provided Below option is selected in Step 6)* In the User ID field, enter the User ID setting from Cisco Unified MeetingPlace.

Step 8 Under Service Capabilities, check the applicable check boxes:

- **MeetingPlace Scheduling and Joining**—Check this check box so that the user can schedule and join meetings.

- **Primary Meeting Service**—If the MeetingPlace Scheduling and Joining check box is checked for two or more unified messaging services, check this check box so that Cisco Unified MeetingPlace meetings will be set up through this Cisco Unified MeetingPlace server. Uncheck this check box so that Cisco Unified MeetingPlace meetings will be set up through another server.

Step 9 Select **Save**.

Step 10 To check the calendar configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace, Cisco Unity Connection, and the user.

Step 11 Repeat Step 2 through Step 10 for all remaining users.

Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration

Do the following procedure.

To Test the Configuration for the Cisco Unified MeetingPlace Calendar Integration

Step 1 Sign in to Cisco Unified MeetingPlace as an end user.

Step 2 Select **Schedule**.

Step 3 Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

Step 4 Sign in to the Connection mailbox of the user that you invited to the Cisco Unified MeetingPlace meeting in Step 3.

Step 5 If the user account is configured for voice recognition, say **Play Meetings**.

If the user account is not configured for voice recognition, press **6**, and then follow the prompts to list meetings.

Step 6 When you hear the system announce the Cisco Unified MeetingPlace meeting that you just scheduled, either say **Join**, or press the applicable keys on the phone keypad to join the meeting.

INDEX

U

V

W