Unified Messaging Guide for Cisco Unity Connection Release 14

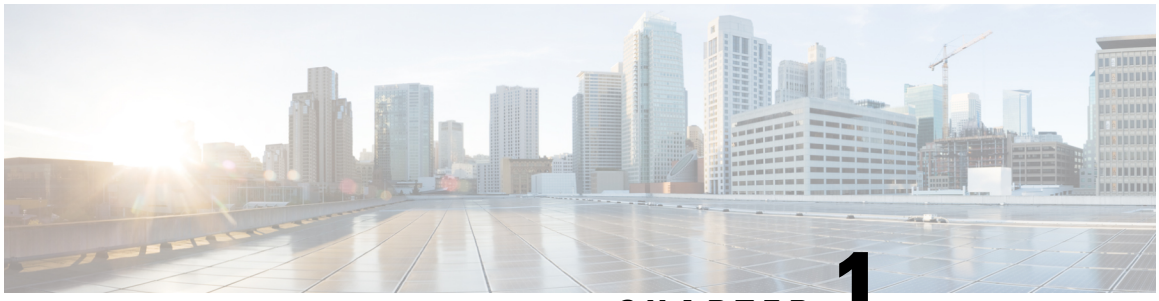
First Published: 2020-11-24

Last Modified: 2021-03-31

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

CONTENTS

CHAPTER 2



CHAPTER 1

Introduction to Unified Messaging

Overview

The unified messaging feature provides a single storage for different types of messages, such as voicemails and emails that are accessible from a variety of devices. For example, a user can access a voicemail either from the email inbox using computer speakers or directly from the phone interface.

The following are the supported mail server with which you can integrate Unity Connection to enable unified messaging:

- Microsoft Exchange (2010, 2013, 2016 and 2019) servers
- Microsoft Office 365
- Cisco Unified MeetingPlace
- Gmail Server

Integrating Unity Connection with an Exchange or Office 365 server provides the following functionalities:

- Synchronization of voicemails between Unity Connection and Exchange/ Office 365 mailboxes.
- Text-to-speech (TTS) access to Exchange/ Office 365 email.
- Access to Exchange/ Office 365 calendars that allows users to do meeting-related tasks by phone, such as, hear a list of upcoming meetings and accept or decline meeting invitations.
- Access to Exchange/ Office 365 contacts that allows users to import Exchange/ Office 365 contacts and use the contact information in personal call transfer rules and when placing outgoing calls using voice commands.
- Transcription of Unity Connection voicemails.

Integrating Unity Connection with Cisco Unified MeetingPlace provides the following functionalities:

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

Integrating Unity Connection with Gmail Server provides the following functionalities:

- Synchronization of voicemails between Unity Connection and Gmailboxes.
- Text-to-speech (TTS) access to Gmail.
- Access to Gmail calendars that allows users to do meeting-related tasks by phone, such as, hear a list of upcoming meetings and accept or decline meeting invitations.
- Access to Gmail contacts that allows users to import Gmail contacts and use the contact information in personal call transfer rules and when placing outgoing calls using voice commands.
- Transcription of Unity Connection voicemails.

Unified Messaging with Google Workspace

Unity Connection 14 and later provides a new way to users for accessing the voice messages on their Gmail account. For this, you need to configure unified messaging with Google Worspace to synchronize the voice messages between Unity Connection and Gmail server.

Integrating Unity Connection with Gmail server provides the following functionalities:

- Synchronization of voicemails between Unity Connection and mailboxes
- Transcription of Unity Connection voicemails.

Single Inbox for Exchange/Office 365

The synchronization of user messages between Unity Connection and supported mail servers is known as Single Inbox. When the single inbox feature is enabled on Unity Connection, voice mails are first delivered to the user mailbox in Unity Connection and then the mails are replicated to the user mailbox on supported mail servers. For information on configuring the Single Inbox in Unity Connection, refer Configuring Unified Messaging chapter.

Note

- The single inbox feature is supported with both IPv4 and IPv6 addresses.
- When the single inbox feature is enabled for a user, the Outlook rules may not work for single inbox messages.
- To see the maximum number of users supported for Exchange and Office 365 server, see the section "Specification for Virtual Platform Overlays" of the *Cisco Unity Connection 14 Supported Platform* List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.html.

Storing Voicemails for Single Inbox Configuration

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

Single Inbox with ViewMail for Outlook

Consider the following points if you want to use Outlook for sending, replying, and forwarding voicemails and to synchronize the messages with Unity Connection:

- Install ViewMail for Outlook on user workstations. If ViewMail for Outlook is not installed, the voicemails that are sent by Outlook are treated as .wav file attachments by Unity Connection. For more information on installing ViewMail for Outlook, see the *Release Notes for Cisco ViewMail for Microsoft Outlook* for the latest release at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
- Make sure to add SMTP proxy addresses for unified messaging users in Unity Connection. The SMTP proxy address of a user specified in Cisco Unity Connection Administration must match the Exchange/ Office 365 email address specified in the unified messaging account in which single inbox is enabled.
- Associate an email account of each user in the organization with a Unity Connection server domain.

The Outlook Inbox folder contains both voicemails and the other messages stored in Exchange/ Office 365. The voicemails also appear in the Web Inbox of a user.

A single inbox user has a **Voice Outbox** folder added to the Outlook mailbox. Unity Connection voicemails sent from Outlook do not appear in the Sent Items folder.

Note Private messages cannot be forwarded.

Single Inbox without ViewMail for Outlook or with Other Email Clients

If you do not install ViewMail for Outlook or use another email client to access Unity Connection voicemails in Exchange/ Office 365:

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

Accessing Secure Voicemails in the Exchange/ Office 365 Mailbox

To play secure voicemails in the Exchange/ Office 365 mailbox, users must use Microsoft Outlook and Cisco ViewMail for Microsoft Outlook. If ViewMail for Outlook is not installed, users accessing secure voicemails see only text in the body of a decoy message which briefly explains the secure messages.

Transcription of Voicemails Synchronized Between Unity Connection and Exchange/Office 365

A system administrator can enable the single inbox transcription functionality by configuring the unified messaging services and the SpeechView transcription services on Unity Connection. "Synchronization of multiple forward messages" service is not supported with Unity Connection, if configured with Single Inbox.

For information on configuring unified messaging services in Unity Connection, refer chapter "Configuring Unified Messaging". For information on configuring SpeechView transcription service, see the "SpeechView" chapter of the *System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

1. In Single Inbox, the transcription of voicemails is synchronized with Exchange in the following ways:
   - When sender sends voicemail to a user through Web Inbox or touchtone conversation user interface and the user views voicemail through various email clients, then the transcription of voicemails are synchronized as shown in the Table 1.

     When Sender Sends Voice Mail through Web Inbox or Touchtone Conversation User Interface

Table 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 voicemails	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 is blank .text.	The **"Transcription in Progress"** text gets displayed in the transcription panel.

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

  When Sender Sends Voicemaill through ViewMail for Outlook

Table 2: When Sender Sends Voicemaill through ViewMail for Outlook

Scenarios	Web Inbox	Outlook WebMail Access/ Outlook without VMO	ViewMail for Outlook
Successful delivery of voicemails	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.
Failure or Response Time-out	The **"Failure or Response Timeout"** text gets displayed in the reading pane of the email.	The **"Failure or Response Time-out"** text is the part of transcript file "Trancription.txt" attached in the voicemail.	The **"Failure or Response Time-out"** text is the part of transcript file "Trancription.txt" attached in the voicemail 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 The message body of the voicemails composed using ViewMail for Outlook and received by Unity Connection are either blank or contain text.

- When a sender sends a voicemail to Unity Connection through third party email clients, the receiver can view the voicemail through various clients after synchronizing the transcription of voicemails.

Do the following steps to synchronize the new voicemails between Unity Connection and mailboxes for a unified messaging user with SpeechView transcription service:

a. Navigate to Cisco Personal Communications Assistant and select **Messaging Assistant**.

b. In the Messaging Assistant tab, select **Personal Options** and enable the **Hold till transcription received** option.

Note By default, the **Hold till transcription received** option is disabled for Exchange/Office 365.

c. The **Hold till transcription received** option enables the synchronization of voicemail between Unity Connection and mail server only when Unity Connection receives time-out/ failure transcription response from the third party external service.

Transcription of Voicemails in Secure and Private Messages

- **Secure Messages**: The secure messages are stored only on the Unity Connection server. 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.

Synchronization with Outlook Folders

The voicemails of a user are visible in the Outlook Inbox folder. Unity Connection synchronizes voicemails in the following Outlook folders with the Unity Connection Inbox folder for the user:

- 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 voicemails (except secure voicemails) into Outlook folders that are not under the Inbox folder, the messages are moved to the deleted items folder in Unity Connection. However, the messages can still be played using ViewMail for Outlook because a copy of the message 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 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 in the deleted items folder in Unity Connection, the message is still playable in Outlook but not resynchronized into Unity Connection.

Unity Connection synchronizes voicemails in the Sent Items folder of Outlook with the Exchange/ Office 365 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 Unity Connection to Exchange/ Office 365 only on an hourly basis.When a user sends a voicemail from Unity Connection to Exchange/ Office 365 or vice versa, the voicemail in the Unity Connection Sent Items folder remains unread and the voicemail in the Exchange/ Office 365 Sent Items folder is marked as read.

By default, the synchronization of voicemails in the Exchange/ Office 365 Sent Items folder with the Unity Connection Sent Items folder is not enabled.

Enabling the Sent Items Folder Synchronization

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

If a user moves a secure message to an Outlook folder that is not synchronized with the Unity Connection Inbox folder, only the copy of the voicemail is moved to the Deleted Items folder in Unity Connection. Such secure messages cannot 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 exists in the Deleted items folder in Unity Connection, the message is synchronized back into the Unity Connection Inbox of the user and the message becomes playable again in Outlook.
- If the message does not exisit in the Deleted items folder in Unity Connection, the message is not resynchronized into Unity Connection and can no longer be played in Outlook.

Step 1 In Cisco Unity Connection Administration, expand System Settings > Advanced, select Messaging.

Step 2 On the Messaging Configuration page, enter a value greater than zero in the Sent Messages: Retention Period (in Days) field.

Step 3 Select Save.

Note When a user sends the voicemail to the Exchange/ Office 365 voice mailbox, the voicemail is not synchronized with the Sent Items folder in Exchange/ Office 365 server. The voicemail remains in the Unity Connection Sent Items folder.

Working of Message Routing Using SMTP Domain Name

Unity Connection uses SMTP domain name to route messages between digitally networked Unity 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 Unity Connection is different from the Corporate Email domain to avoid issues in message routing for 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 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 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 section

Location for Deleted Messages

By default, when a user deletes a voicemail 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 (you can either do this manually or configure message aging to do it automatically), it is also deleted from the Outlook Deleted Items folder.

When a user deletes a voicemail from any Outlook folder, the message is not permanently deleted but it is moved to the Deleted Items folder. No operation in Outlook causes a message to be permanently deleted in Unity Connection.

To permanently delete messages using Web Inbox or Unity Connection phone interface, you must configure Unity Connection to permanently delete messages without saving them in the Deleted Items folder.

When Unity Connection synchronizes with Exchange/ Office 365, the message is moved to the Unity Connection Deleted items folder but not permanently deleted.

Note We can also permanently delete messages from the Unity Connection Deleted Items folder using Web Inbox.

To permanently delete messages from the Unity Connection Deleted Items folder, do either or both of the following steps:

- 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.

Types of Messages Not Synchronized with Exchange/ Office 365

The following types of Unity Connection messages are not synchronized:

- Draft messages
- Messages configured for future delivery but not yet delivered

- Broadcast messages
- Unaccepted dispatch messages

Note When a dispatch message is accepted by a recipient, it becomes a normal message and is synchronized with Exchange/ Office 365 for the user who accepted it and deleted for all other recipients. Until someone in the distribution list accepts a dispatch message, the message waiting indicator for everyone in the distribution list remains on, even when users have no other unread messages.

Affect of Disabling and Re-enabling Single Inbox

When you configure unified messaging, you can create one or more unified messaging services. Each unified messaging service has a set of specific unified messaging features enabled. You can create only one unified messaging account for each user and associate it with a unified messaging service.

Single inbox can be disabled in the following 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 using any of these methods, Unity Connection resynchronizes the Unity Connection and Exchange/ Office 365 mailboxes for the affected users. Note the following:

- If users delete messages in Exchange/ Office 365 but do not delete the corresponding messages in Unity Connection while single inbox is disabled, the messages gets resynchronized into the Exchange mailbox when single inbox is re-enabled.
- If messages are hard deleted from Exchange/ 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 Unity Connection when single inbox is re-enabled are resynchronized into the Exchange/ Office 365 Deleted Items folder.
- If users hard delete the messages in Unity Connection but do not delete the corresponding messages in Exchange/ Office 365 while single inbox is disabled, the messages remain in Exchange/ Office 365 when single inbox is re-enabled. Users must delete the messages from Exchange/ Office 365 manually.
- If users change the status of messages in Exchange/ Office 365 (for example, from unread to read) while single inbox is disabled, the status of Exchange/ Office 365 messages is changed to the current status of the corresponding Unity 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 Unity Connection and Exchange/ Office 365 mailboxes, resynchronization for existing messages may affect synchronization performance for new messages.

- When you re-enable single inbox, depending on the number of users associated with the service and the size of their Unity Connection and Exchange/ Office 365 mailboxes, resynchronization for existing messages may affect synchronization performance for new messages.

Synchronization of Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts

Unity Connection can send read/heardreceipts, delivery receipts, and non-delivery receipts to Unity Connection users who send voicemails. If the sender of a voicemail is configured for single inbox, the applicable receipt is sent to the Unity Connection mailbox of the sender. The receipt is then synchronized into the Exchange/ Office 365 mailbox of the sender.

Note the following.

- ***Read/heard receipts:*** When sending a voicemail, a sender can request a read/heard receipt.

  Do the following steps to prevent Unity Connection to respond to requests for read receipts:

  - In Unity Connection Administration, either expand **Users** and select **Users**, or expand **Templates** and select **User Templates**.
  - If you selected **Users**, then select an applicable user and open the Edit User Basics page. If you selected **User Templates**, then select an applicable template and open the Edit User Template Basics page.
  - On the Edit User Basics page or the Edit User Template Basics page, select **Edit** > **Mailbox**.
  - On the Edit Mailbox page, uncheck the **Respond to Requests for Read Receipts** check box.

- ***Delivery receipts:*** A sender can request a delivery receipt only when sending a voicemail 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 voicemail cannot be delivered.

  Do the following steps to prevent Unity Connection to send an NDR when a message is not delivered:

  - In Unity Connection Administration, either expand **Users** and select **Users**, or expand **Templates** and select **User Templates**.
  - If you selected **Users**, then select an applicable user and open the Edit User Basics page. If you selected **User Templates**, then select an applicable template and open the Edit User Template Basics page.
  - On the Edit User Basics page or the Edit User Template Basics page, uncheck the**Send Non-Delivery Receipts for Message Failed Delivery** check box and select Save.

Note

- When the sender accesses Unity Connection using the TUI, the NDR includes the original voicemail that allows the sender to resend the message at a later time or to a different recipient.
- When the sender accesses Unity Connection using Web Inbox, the NDR includes the original voicemail but the sender cannot resend it.
- When the sender uses ViewMail for Outlook to access Unity Connection voicemails that have been synchronized into Exchange, the NDR is a receipt that contains only an error code, not the original voicemail, so the sender cannot resend the voicemail.
- 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.

Single Inbox with Google Workspace

The synchronization of user messages between Unity Connection and Gmail mail server is known as Single Inbox. When the single inbox feature is enabled on Unity Connection, voice mails are first delivered to the user mailbox in Unity Connection and then the mails are replicated to the Gmail account of the user. For information on configuring the Single Inbox in Unity Connection, refer Configuring Unified Messaging, on page 15 “Configuring Unified Messaging” chapter.

Note

- The single inbox feature with Google Workspace is supported with both IPv4 and IPv6 addresses.
- To see the maximum number of users supported for Google Workspace, see the section “Specification for Virtual Platform Overlays” of the *Cisco Unity Connection 14 Supported Platform* List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.html.

Single Inbox with Gmail Client

If you do not install ViewMail for Outlook or use another email client to access Unity Connection voicemails in Exchange/ Office 365/Gmail server:

- The Gmail client treats voicemails as emails with .wav file attachments.
- When a user replies to or forwards a voicemail, the reply or forward also is treated as an email even if the user attaches a .wav file. Message routing is handled by Gmail server, not by Unity Connection, so the message is never sent to the Unity Connection mailbox for the recipient.
- Users cannot listen to secure voicemails.
- It may be possible to forward private voicemails.

Accessing Secure Voicemails

To play secure vocemails when Google Worspace is configured, users must use Telephony User Interface (TUI). The users accessing secure voicemails on Gmail account see only text message which indicates that message is secured and can be listen through TUI.

Transcription of Voicemails Synchronized Between Unity Connection and Gmail Server

A system administrator can enable the single inbox transcription functionality by configuring the unified messaging services and the SpeechView transcription services on Unity Connection. "Synchronization of multiple forward messages" service is not supported with Unity Connection, if configured with Single Inbox.

For information on configuring unified messaging services in Unity Connection, refer chapter "Configuring Unified Messaging". For information on configuring SpeechView transcription service, see the "SpeechView" chapter of the *System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

In Single Inbox, the transcription of voicemails is synchronized with Gmail server when sender sends voicemail to a user through Web Inbox or touchtone conversation user interface and the user views voicemail through Gmail client, then the transcription of voicemails are synchronized as below:

- For successful delivery of voicemails, the text of the transcription gets displayed in the reading pane of the email.
- For failure or response time-out, the "Failure or Response Timeout" text gets displayed in the reading pane of the email.

Do the following steps to synchronize the new voicemails between Unity Connection and Google Workspace mailboxes for a unified messaging user with SpeechView transcription service:

1. Navigate to Cisco Personal Communications Assistant and select **Messaging Assistant**.
2. In the Messaging Assistant tab, select **Personal Options** and enable the **Hold till transcription received** option.

Note By default, the **Hold till transcription received** option is disabled.

3. The **Hold till transcription received** option enables the synchronization of voicemail between Unity Connection and Google Workspace only when Unity Connection receives response from the third party external service.

Text-to-Speech

The Text-to-Speech feature allows the unified messaging users to listen to their emails when they sign in to Unity Connection using phone.

Unity Connection supports text-to-speech feature with the following mailbox stores:

- Office 365

- Exchange 2016
- Exchange 2019

Note Text-to-Speech over Office 365, Exchange 2016, Exchange 2019 supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Unity Connection platform is compatible and configured in dual (IPv4/IPv6) mode.

Unity Connection can be configured to deliver transcriptions to an SMS device as a text message or to an SMTP address as an email message. The fields to turn on transcription delivery are located on the SMTP and SMS Notification Device pages where you set up message notification. For more information on notification devices, see the "Configuring Notification Devices" section in the "Notifications" chapter of the *System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Following are the considerations for effective use of transcription delivery:

- In the **From** field, enter the number you dial to reach Unity Connection when you are not dialing from the desk phone. If you have a text-compatible mobile phone, can initiate a callback to Unity Connection in the event that you want to listen to the message.
- You must check the **Include Message Information in Message Text** check box to include call information, such as caller name, caller ID (if available), and the time that the message was received. If the check box is unchecked, the message received does not indicate the call information.

In addition, if you have a text-compatible mobile phone, you can initiate a callback when the caller ID is included with the transcription.

- In the **Notify Me Of** section, if you turn on notification for voice or dispatch messages, you are notified when a message arrives and the transcription soon follows. If you do not want notification before the transcription arrives, do not select the voice or dispatch message options.
- Email messages that contain transcriptions have a subject line that is identical to notification messages. So, if you have notification for voice or dispatch messages turned on, you have to open the messages to determine which one contains the transcription.

Note For information on configuring the text-to-speech feature in Unity Connection, see the Configuring Text-to-Speech chapter.

Calendar and Contact Integration

Note For information on configuring calendar and contact integration in Unity Connection, see the Configuring Calendar and Contact Integration chapter.

About Calendar Integration

The calendar integration feature enables the unified messaging users to do the following tasks over 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).

Unity Connection supports calendar applications when integrated with the following mail servers:

- Office 365
- Exchange 2016
- Exchange 2019

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, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user/guide/phone/b_14cucugphone.html.

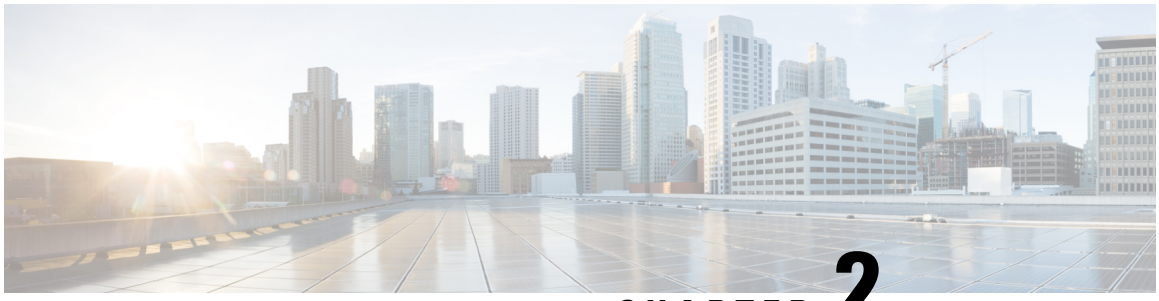
For using Personal Call Transfer Rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user/guide/pctr/b_14cucugpctr.html.

About Contact Integrations

Unity Connection allows users to import Exchange contacts and use the contact information in Personal Call Transfer Rules and when placing outgoing calls using voice commands. Unity Connection supports contact applications when integrated with the following mail servers:

- Office 365
- Exchange 2016
- Exchange 2019

For importing Exchange contacts, see the "Managing Your Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user/guide/assistant/b_14cucugasst.html.



CHAPTER 2

Configuring Unified Messaging

Cisco Unity Connection can be integrated with Microsoft Exchange 2019, 2016, Office 365 and Gmail Server to deploy the unified messaging feature.

Overview of Unity Connection Communication with Exchange Server

When you add a unified messaging service that defines the communication between Unity Connection and Exchange, you can select 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 select a specific Exchange 2016 client access server, Unity Connection can access all Exchange 2016 mailboxes in the Exchange organization, but cannot access Exchange 2019 mailboxes.
- If you select a specific Exchange 2019 client access server, Unity Connection can access all Exchange 2019, and Exchange 2016 mailboxes in the Exchange organization.
- If you allow Unity Connection to search for Exchange servers, you need to give permissions to the Exchange servers. See the below section to grant permissions to the applicable Exchange server:

Granting Permissions for Exchange 2013, Exchange 2016 or Exchange 2019, on page 26

Note If you want to select 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 mailboxes in the Exchange organization. Table 1 explains when you need to add more than one unified messaging service.

Table 3: Adding Unified Messaging Services Based on Versions of Exchange

Exchange Versions with Mailboxes That You Want Unity Connection to be Able to Access			
Exchange 2016	Exchange 2019	Office 365	Create the Following Unified Messaging Services
No	No	Yes	One for Office 365 server that you want Unity Connection to be able to access.
No	Yes	Yes	• One for Exchange 2019. • One for Office 365 server that you want Unity Connection to be able to access.
Yes	Yes	Yes	• One for Exchange 2019. This service can also access Exchange 2016 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access.
Yes	Yes	Yes	• One for Exchange 2019. This service can also access Exchange 2016 mailboxes. • One for Office 365 server that you want Unity Connection to be able to access.
Yes	No	Yes	• One for Exchange 2016. • One for Office 365 server that you want Unity Connection to be able to access.
Yes	No	No	One for Exchange 2016.

Exchange Versions with Mailboxes That You Want Unity Connection to be Able to Access			
Yes	No	Yes	• One for Exchange 2016. • One for Office 365 server that you want Unity Connection to be able to access.
No	No	Yes	• One for Office 365 server that you want Unity Connection to be able to access.

- If you select to allow Unity Connection to search for Exchange servers, Unity Connection automatically detects when you move mailboxes from one version of Exchange to another, and automatically update Unity Connection user settings.
- If you select a specific Exchange server, Unity Connection sometimes detects when you move mailboxes from one Exchange server to another, and automatically access the Exchange mailbox in new location. When Unity Connection cannot detect the new mailbox, you must manually update unified messaging services or unified messaging accounts:
  - *If you moved all 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 identifies when Unity Connection 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 and Restoring Exchange Mailboxes" chapter.

Table 4: Choosing a Specific Exchange Server: When Unity Connection Detect Moving a Mailbox Between Exchange Servers

If you select a specific	Unity Connection can automatically detect mailbox moves between the following Exchange versions				
	2016	**2019**	**2016 and 2016**	**2016 and 2019**	**2019 and 2019**
Exchange 2016 server	Yes	No	Yes	No	No
Exchange 2019 server	Yes	Yes	Yes	Yes	Yes

If Unity Connection is not configured to use DNS, you must select a specific Exchange server. If this does not allow you to access all the Exchange mailboxes in the organization as described earlier in this section, you must create more than one unified messaging service.

If you select a specific Exchange server and that server stops functioning, Unity Connection cannot access any Exchange mailboxes. If you select 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.

Unified Messaging with Google Workspace

Unity Connection 14 and later provides user a new way to access the emails and voice messages on the Gmail account of the user. It allows administrator to integrate unified messaging with Google Workspace. Using Google Workspace, you can configure Unity Connection to synchronize voice messages between Unity Connection and Gmail Server. All Unity Connection voice messages that are sent to user, are first stored in Unity Connection and then synchronized to the user's Gmail account.

Prerequisites for Configuring Unified Messaging

Following prerequisites should be met before configuring Unified Messaging:

1. Review the "Requirements for Using Unified Messaging Features" section in the System Requirements for Cisco Unity Connection Release 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html
2. If *Unity Connection is integrated with an LDAP directory* : Navigate to Cisco Unity Connection Administration and verify the following:
   - Expand **System Settings** and select **LDAP Directory Configuration**. Select the applicable LDAP directory configuration. On the LDAP Directory Configuration page, make sure the **Mail ID** field in **Cisco Unified Communications Manager User Fields** is synchronized with the mail in **LDAP Attribute**.

     This causes values in the **LDAP mail** field to appear in the **Corporate Email Address** field of the LDAP imported user.
   - Expand **Users** and select **Users**. Select the applicable user. On the Edit User Basics page, enter the **Corporate Email Address**.
   - Select **Edit** on the user page and then select **Unified Messaging Account**. On the Unified Messaging Account page of the user, make sure value in the **Email Address** field is specified.

Task List for Configuring Unified Messaging

Task List for Configuring Unified Messaging with Exchange 2013, Exchange 2016 or Exchange 2019

Step 1 Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

Step 2 Create an Active Directory account for unified messaging users to communicate with Exchange 2013, Exchange 2016 or Exchange 2019. For more information on creating unified messaging services account in Active Directory and granting permissions, see the Configuring Unified Messaging in Active Directory section.

Step 3 Decide whether you want Unity Connection to be able to search for and communicate with different Exchange 2013, Exchange 2016 or Exchange 2019 server, or you want Unity Connection to communicate with a specific Exchange 2013, Exchange 2016 or Exchange 2019 server in case the hostname or the IP Address of the specific server is known. Do the following steps:

a) Granting Permissions for Exchange 2013, Exchange 2016 or Exchange 2019

b) *(Optional)* Confirming Exchange 2013, Exchange 2016 or Exchange 2019 Authentication and SSL Settings

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

Step 4 If Unity Connection is not configured to use DNS, use the following CLI commands to configure DNS:

- **set network dns**
- **set network dns options**

Note 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.

Step 5 *(Selected configurations only)*: In either or both of the following conditions, you need to 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 have configured Exchange to use HTTPS in Step 3 b, configure unified messaging services to validate certificates for Exchange servers.
- If you have 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.

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 username 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, you must configure unified messaging services to communicate with Active Directory domain controllers using the secure LDAP (LDAPS) protocol.

For more information, see the Uploading CA Public Certificates for Exchange and Active Directory section.

Step 6 Configure one or more unified messaging services on Unity Connection. For more information, see theGranting Permissions section.

Step 7 Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

Step 8 Configure one or more unified messaging accounts to link the Unity Connection users with the mail server with which they are communicating. For more information, see the Unified Messaging Account for Users section.

Step 9 Test unified messaging configuration. For more information, see the Test Unified Messaging Configuration section.

Task List for Configuring Unified Messaging with Office 365

Step 1 Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

Step 2 Create an Active Directory account to be used by Unity Connection unified messaging users to communicate with Office 365. For more information on creating unified messaging services account in Active Directory and granting permissions, see the Configuring Unified Messaging in Active Directory section.

Step 3 Decide and select the type of authentication that you want Unity Connection to use to sign in to Office 365 client access servers. To do this, navigate to **Unified Messaging** > **Unified Messaging Services** on Cisco Unity Connection Administration and select **Add New**. On the New Unified Messaging Service page, select either of the following from **Web-Based Authentication Mode** field:

- **Basic**: Default authentication mode.
- **NTLM**: Before switching to NTLM authentication mode, make sure that the same mode is configured on the Office 365 server.
- **OAuth2** : OAuth 2.0 based authentication mode.

Note Basic authentication has been deprecated by Microsoft

Cisco Unity Connection supports **OAuth2** authentication mode for configuring Unified Messaging with Office 365. For using OAuth2 web authentication mode, you must create and register an application on Microsoft Azure portal corresponding to the Unified Messaging Service. For more information, see Step 4.

For existing Unified Messaging Service, select the above settings on Edit Unified Messaging Service page.

Step 4 *(Applicable only for OAuth2 web authentication mode)* Refer the following steps for registering the application on Azure portal.

Note The steps may be changed or modified as per the latest updates available from Microsoft.

a) Sign in to Azure portal global endpoint at portal.azure.com with Azure portal Administrator to create Unified Messaging Service account. For other applicable Azure portal endpoints, refer section **App registration endpoints** in microsoft documentation available at link https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud

b) On the portal, select **Azure Active Directory**. A new window of Azure Active Directory appears.

c) On Azure Active Directory window, select **App registrations** and create a new application using **New registration** field. After successfully registering the application, you get the values of **Application (Client) ID** and **Directory ID** that are used for configuring Unified Messaging.

d) Select **Certificates & secrets** and create a new **Client Secret** that provides a Client Secret value, used for configuring Unified Messaging.

Note Make sure to copy the value of Client secret at the time of creation otherwise you have to create a new Client Secret for the application.

e) Select **API permissions** > **Add a permission** > **APIs my organization uses**. Enter **Office 365 Exchange Online** in search bar and select it.

f) *(Applicable to 14SU2 and earlier releases)* Click **Delegated permissions** and add below permissions in your application:

Features	Permissions
EWS	EWS.AccessAsUser.All

Features	Permissions
Mail	Mail.ReadWrite, Mail.Send

For accessing Calendar and Contacts, you should also add below permissions in your application:

Features	Permissions
Calendars	Calendars.ReadWrite
Contacts	Contacts.ReadWrite

g) *(Applicable to 14SU3 and later releases)* Click **Application permissions** and add **full_access_as_app** permission in your application. To restrict the permissions, see steps mentioned inTask List for restricting Application Permissions to mailboxes, on page 23.

h) On API permissions window, select **Grant admin consent for Cisco Systems** to provide grant admin consent for the requested permissions.

For more information on registering Application on Azure portal, see https://docs.microsoft.com/en-us/graph/auth-register-app-v2.

Step 5 *(Applicable only for OAuth2 web authentication mode)* Enter the values of below fields getting from the Azure portal in step 4:

- **Application (Client) ID.**
- **Directory ID.**
- **Client Secret.**
- **AD Authentication Endpoint.** Its default value is https://login.microsoftonline.com.

  Note For other applicable AD Authentication Endpoints refer section **Azure AD authentication endpoints** in Microsoft documentation available at link https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud

- **Resource URI.** Its default value is https://outlook.office365.com.

Note Repeat Steps 4 and 5 for the following:

- In case of multiple clusters , the above fields should be unique for each cluster configuration.
- When configuring multiple Unified Messaging services in Unity Connection you must create a unique Client ID for each service.

Step 6 *(Applicable to 14SU2 and earlier releases)* Do the following tasks on the Office 365 server to enable Auto Discovery functionality that enables Unity Connection to search for and communicate with different Office 365 servers:

a) Accessing Office 365 Using Remote Exchange Management Power Shell

b) (Applicable for 14SU2 and earlier releases) Assigning Application Impersonation Role for Office 365

Note Unity Connection uses the HTTPS protocol to validate certificates based on the settings in the applicable unified messaging service.

Step 7 Synchronization threads configuration should be done based on latency between Unity Connection and Office 365 server. For more information, see the "Latency" section of the “Single Inbox” chapter in the *Design Guide for Cisco Unity Connection Release 14*, available at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/design/guide/b_14cucdg.html

Step 8 Run the following CLI commands to configure DNS:

- **set network dns**
- **set network dns options**

Note 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.

Step 9 (*Selected configurations only*): Upload SSL certificates on the Unity Connection server to encrypt the communication between Unity Connection and Office 365. Uploading certificates allows you to:

- Validate the certificates for Exchange Servers. To do this, check the **Validate Certificates for Exchange Servers** check box on Unity Connection Administration.
- Secure communication when you have configured Unity Connection to search for and communicate with Office 365 servers.

For more information, see the Uploading the Public Certificates to the Unity Connection Server and Uploading Certificates for Office 365 and Cisco Unity Connection

Step 10 Create one **Unified Messaging Service** and configure all the users with that service account.

Note If Unity Connection server is being shared by tenants for voicemail service, then multiple **Unified Messaging Service** accounts are required.

Step 11 Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

Step 12 Run the following CLI commands to configure the number of users aggregated per streaming thread and hourly periodic full resynchronization flag for mailbox synch.

a) Check the existing number of users.

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchUserCountPerStreamingSubscription'
```

If "value" parameter is 5000, it means configuration is already enabled. If value is not 5000, run the below CLI command to set the number of users.

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyLong(pFullName='System.Messaging.MbxSynch.MbxSynchUserCountPerStreamingSubscription',pvalue=5000)
```

b) Check the existing configuration of the hourly periodic full resynchronization flag for mailbox synch.

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchBackgroundSyncEnable'
```

If "value" parameter is 0, it means the configuration is already enabled.If value is not 0, run the below CLI command to set the flag.

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchBackgroundSyncEnable',pvalue=0)
```

c) You must restart **Connection Mailbox Sync** service for above CLI changes to come into effect.

Note In case of cluster, execute the commands only on publisher server and after that make sure that database replication is working fine.

Step 13 Test the unified messaging service. For more information, see the Test Unified Messaging Configuration

Task List for restricting Application Permissions to mailboxes

Step 1 Create a **mail-enabled security group**. It can be used to distribute messages and to grant access permissions to resources in Active Directory. See steps available at https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-mail-enabled-security-groups#use-the-exchange-admin-center-to-manage-a-mail-enabled-security-group.

Step 2 Install the **Exchange Online Management Module** in an elevated Powershell. See steps available at https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exchange-online-powershell-module.

Step 3 Connect to **Exchange Online PowerShell**. See steps available at https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps.

Step 4 Run the **New-ApplicationAccessPolicy** cmdlet. For running New-ApplicationPolicy, **OrganizationConfiguration** Role is required. You can check the current Role by the following command:

```
Get-ManagementRole -Cmdlet <Cmdlet>
```

Do the following steps for assigning OrganizationConfiguration role to the admin user :

a) Login Exchange Admin Center at https://admin.exchange.microsoft.com/.

b) Select **Roles → Admin Roles**.

c) Select **Organization Management** role for the user.

d) Restart Power Shell to make sure the new role assignment is in effect

Step 5 Run the **New-ApplicationAccessPolicy** cmdlet by the following command:.

```
New-ApplicationAccessPolicy -AppId "**" -PolicyScopeGroupId "**" -AccessRight RestrictAccess
-Description "Restrict this app to members."
```

Note AppId is the Application Id of the Application for which you want to restrict the access. It will be the client id mentioned in Azure Active Directory Portal for the application. You can also provide multiple appid's separated by commas. PolicyScopeGroupId is Id to identify the group. It will be the Mail enabled security group mentioned in **Step 1**.

Note The steps may be changed or modified as per the latest updates available from Microsoft.

Task List for Configuring Unified Messaging with Google Workspace

Gmail API provides server push notifications through which, user examine the changes in user mailbox on Gmail server. Whenever there is a change in user mailbox, Gmail API sends notification to Unity Connection.

Step 1 Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

Before configuring unified messaging with Google Workspace, you must have domain name to create an account on Google Workspace.

Step 2 Go to Google Workspace and create an account on Admin Console using domain name. For detailed step, see https://workspace.google.com/signup/businessstarter/welcome?hl=en-IN.

Step 3 Go to Google Cloud Platform (GCP) Console and login to Google Cloud Console with administrator account created in Step 2 and create a new Project.

The project specifies the domain that is used to create a service account.

Step 4 On Google Cloud Platform, to create a new project, select **NEW PROJECT** option from the drop-down menu of the organization domain and enter the required information and select **CREATE**.

Step 5 After creating the project, select your project from the drop-down menu of the organization domain.

Step 6 On the project home page, navigate Menu > IAM & Admin > Service accounts > Create service account.

Step 7 On Create Service Account page, enter the required information and select **CREATE AND CONTINUE**.

Step 8 To provide all the permissions to the sevice account, select **Owner** role from the drop-down menu of **Role** under **Grant this sevice account access to project** field.

Step 9 Select **DONE**.

A new page opens with all sevice accounts created under the project.

Step 10 Select the service account created in Step 7.

Step 11 On the sevice account page, go to **DETAILS** tab and select **SHOW DOMAIN-WIDE DELEGATION** field and check the **Enable Google Workspace Domain-wide Delegation** check box to allow service account to access all users data on a Google Workspace domain.

Step 12 Select **SAVE**.

Step 13 On the sevice account page, go to **KEYS** tab and select **ADD KEY** > **Create new key**.

Make sure to select JSON option in **Key type** field.

After successfully created the account, key file in .json format is downloaded on the system. The key file is used for configuring unified messaging with Google Workspace.

Step 14 Navigate to **Menu** > **API & Services** > **Library** and search for Gmail API and enable it.

Similarly, search for Cloud Pub/Sub API and enable it.

Step 15 To delegate domain-wide authority to Service Account, navigate Menu > IAM & Admin > Service accounts and select **View Client ID** corresponding to the service account created and copy the Client ID.

Step 16 Log in to Admin Console and navigate Menu > Security > API controls.

Step 17 On API controls page, select Domain-wide Delegation and select Add new.

Step 18 A new window appears to enter the client ID.

Step 19 On Add a new client ID window, enter the Client ID copied in Step 15 and provide OAuth scopes and select AUTHORIZE.

Scopes required :

https://mail.google.com,

https://www.googleapis.com/auth/gmail.labels,

https://www.googleapis.com/auth/gmail.modify,

https://www.googleapis.com/auth/cloud-platform,

https://www.googleapis.com/auth/pubsub

Step 20 Create users using **Users** application on Admin Console.

Step 21 Login to Cisco Unity Connection Administration, navigate to **Unified Messaging** > **Unified Messaging Services** and select **Add New**.

Step 22 On the New Unified Messaging Service page, select Google Workspace for New Unified Messaging Service.

Step 23 To enable Unified Messaging with Google Workspace feature, check **Enabled** check box.

By default the check box is checked.

Step 24 To enable verification of Google Workspace Certificates , check **Validate Certificates for Google Workspace** check box.

By default the check box is unchecked.

Step 25 Enter display name for new unified messaging service.

Step 26 Enter **Proxy Server (Address:Port)** field for proxy server if required.

Step 27 Check **Enable Proxy Server Authentication** check box to enable proxy server based authentication and provide the **Username** and **Password** for the proxy server.

Step 28 In, **Google Workspace Service Account Key File**, upload key file created in Step 13.

Make sure to upload the file in .json format and its size should be less than 1MB.

Step 29 Select Save.

Step 30 Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

Step 31 Configure one or more unified messaging accounts to link the Unity Connection users with the mail server with which they are communicating. For more information, see the Unified Messaging Account for Users section.

Task for Configuring Unified Messaging

Configuring Unified Messaging in Active Directory

Unity Connection accesses Exchange or Office 365 mailboxes 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 Office 365, Exchange 2019, Exchange 2016 and Exchange 2013 operations are performed through Exchange Web Services (EWS). Uploading messages into Exchange mailboxes

- Tracking changes to messages in Exchange
- Updating messages with changes made in Unity Connection
- Deleting messages in Exchange when the messages are deleted in Unity Connection, and so on.

You need to 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 points while configuring Unified Messaging in active directory:

- Give the account a name that identifies it as the unified messaging services account for Unity Connection.
- Do not create a mailbox for the domain user account. If you create a mailbox for the account, unified messaging does 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 or Office 365 mailboxes.
- Specify a password that satisfies the password-security requirements of your company.

Note 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 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 servers. However, this is not a requirement and does not affect functionality or performance.

Granting Permissions

Granting Permissions for Exchange 2013, Exchange 2016 or Exchange 2019

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

Step 2 Run the following command in Exchange Management Shell to assign the Application Impersonation management role to the unified messaging services account for Exchange 2013, Exchange 2016 or Exchange 2019:

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.

If you have 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, Exchange 2016 or Exchange 2019 you need to assign the Application Impersonation management role to the unified messaging service account.

Confirming Authentication and SSL Settings

After choosing the Exchange server accessed by Unity Connection for unified messaging, confirm that the Exchange servers are configured to use the desired authentication mode (Basic, Digest, or NTLM) and web-based protocol (HTTPS or HTTP).

Unity Connection supports NTLMv2 based authentication when a user selects NTLM authentication mode for configuring unified messaging.

After configuring the authentication mode and web-based protocols on Exchange servers, create one or more Unity Connection unified messaging services. Select the same authentication mode and web-based protocol that you specify in the servers.

Confirming Exchange 2013, Exchange 2016 or Exchange 2019 Authentication and SSL Settings

Step 1 Decide the type of authentication (**Basic** or **NTLM**) you want Unity Connection to use to sign in to Exchange 2013, Exchange 2016 or Exchange 2019 client access servers. You must configure all Exchange 2013, Exchange 2016 or Exchange 2019 client access servers to use the same type of authentication.

Step 2 Decide whether you want the communication between Unity Connection and Exchange 2013, Exchange 2016 or Exchange 2019 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on all the Exchange 2013, Exchange 2016 or Exchange 2019 client access servers.

Step 3 Sign in to a server that has access to the same Exchange 2013 client servers that is accessed by the Unity Connection. 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, Exchange 2016 or Exchange 2019 client access server for which you want to confirm settings, in the left pane, expand <servername> > **Sites** > **Default Website**>. You need to verify the authentication settings for both EWS and Autodiscover.

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

a) In the middle pane, in the **IIS** section, double-click **Authentication**.

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 configure Unity Connection to use the same type of authentication. Unity Connection supports only the following types of authentication:

- **Basic**
- **NTLM**

b) If you have changed any settings, in the right pane, select **Apply**.

c) In the left pane, select **Autodiscover** again.

d) In the middle pane, double-click **SSL Settings**.

e) On the SSL Settings page, if the **Require SSL** check box is checked:

- You must select HTTPS for the web-based protocol while creating a unified messaging service in Unity Connection.
- You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

f) If you changed any settings, in the right pane, select **Apply**.

Step 7 Under **Default Website**, select **EWS**:

a) In the middle pane, in the IIS section, double-click **Authentication**.

Confirm that the **Status** column displays **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 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.

b) If you changed any settings, in the right pane, select **Apply**.

c) In the left pane, select **EWS** again.

d) In the middle pane, double-click **SSL Settings**.

e) If the **Require SSL** check box is checked:

- You must select 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 e.

f) If you have changed any settings, in the right pane, select **Apply**.

Step 8 Repeat Step 5 through Step 6 for the other Exchange 2013, Exchange 2016 or Exchange 2019 client access servers that Unity Connection can access.

Step 9 Close **IIS Manager**.

Configuring Paged View Functionality in Unity Connection for Exchange 2013, Exchange 2016 or Exchange 2019

If any unified user Exchange mailboxes have more than 1000 messages including voicemails and receipts, then enable the EWS paged view search functionality in Unity Connection server.

To enable the paged view functionality for messages, you must set the value of the 'System.Messaging.MbxSynch.MbxSynchUsePaging' parameter to 1.

Do the following to configure paged view functionality:

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

Step 2 To set the maximum limit of voicemails items that can be managed by 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. Unity Connection by default manages the first 25000 voicemails per mailbox which avoids any delay in message synchronization between Unity Connection and Exchange server. This voicemail count limit can be increased maximum up to 75000.

Note By default, the value of the parameter ‘System.Messaging.MbxSynch.MbxSynchUsePaging' parameter is set to 1.

Accessing Office 365 Using Remote Exchange Management Power Shell

Step 1 Run Windows PowerShell as administrator and run the 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 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.

(*Applicable for 14SU2 and earlier releases)* Assigning Application Impersonation Role for Office 365

Step 1 To configure impersonation in Office 365, you must run a Windows PowerShell script.

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

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.

Creating a Unified Messaging Service to Access Mail Server

Do the following procedure to create one or more unified messaging services in Unity Connection to access the supported mail server.

Note If you configured the supported mail server to use HTTPS, you need to configure the unified messaging services to validate certificates for the mail servers. You need to upload certificates from the certification authority that issued the SSL certificates for mail server to both Tomcat-trust and Unity Connection-trust locations. For information on uploading SSL certificates, see the "Using SSL to Secure Client/Server Connections" chapter of the *Security Guide for Cisco Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

Creating Unified Messaging Services in Unity Connection

If you are configuring Unity Connection to communicate with individual mail servers, you need to configure unified messaging services for each mail server.

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

Step 2 On the Search Unified Messaging Services page, select **Add New** to create a new unified messaging services. You may also select an already created unified messaging services and modify its settings. The New Unified Messaging Services page or Edit Unified Messaging services page appears.

Step 3 Enter the values of the required fields to configure unified messaging services and select **Save** (For information on each field, see **Help> This Page** depending on the mail server you selected).

If you are configuring Unity Connection to communicate with individual mail servers, you need to configure unified messaging services for each mail server.

Uploading CA Public Certificates for Exchange and Active Directory

At the time of creating unified messaging services, if you selected 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.

The public certificates allow Unity Connection to communicate with Exchange servers or DCs and unified messaging functions properly.

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 2019, Exchange 2016 or Exchange 2013 client access servers.

   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, 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 Saving the Public Certificate for Microsoft Certificate Services or Active Directory Certificate Services to a File.

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 have downloaded 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. For more information, see the Uploading the Public Certificates to the Unity Connection Server. and Uploading Certificates for Office 365 and Cisco Unity Connection

Saving 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 2019, Exchange 2016 or Exchange 2013 client access servers.
- 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 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 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.

Uploading the Public Certificates to the Unity Connection Server

Step 1 In Cisco Unified Operating System Administration, expand Security and select **Certificate Management**.

Step 2 On the Certificate Management page, select **Upload Certificate**.

Step 3 In the Certificate Name list, select **tomcat-trust**.

Step 4 *(Optional)* Enter a description in the **Description** field and select **Browse**.

Step 5 Browse to the location where you saved the public certificates in .pem format, and select one of the converted certificates.

Step 6 Select **Upload File**.

Step 7 Repeat Step 2 through Step 6, but select **Unity Connection-trust** in the Certificate Name list.

Step 8 If you have public certificates from more than one certification authority, repeat Step 2 through Step 7 for the remaining certificates.

Uploading Certificates for Office 365 and Cisco Unity Connection

At the time of creating unified messaging services, if you select "Validate Certificates for Exchange Servers" for Office 365, you must perform the following steps to upload Office 365 root certificate to the tomcat-trust of Cisco Unity Connection.

Step 1 Select the Office 365 EWS endpoint URL https://outlook.office365.com/EWS/Exchange.ASMX and download the Office 365 root certificate.

Step 2 In Cisco Unified Operating System Administration, expand Security and select Certificate Management.

Step 3 On the Certificate Management page, select Upload Certificate.

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

Step 5 *(Optional)* Enter a description in the **Description** field and select Browse

Step 6 Browse to the location where you saved the Office 365 root certificate, and select the certificate.

Step 7 Select Upload File.

Caution If Office 365 EWS endpoint URL communicates with Cisco Unity Connection through a different root certificate, the same must be uploaded to the tomcat-trust of Cisco Unity Connection.

Settings Configured on Unity Connection Users

Step 1 In Cisco Unity Connection Administration, expand **Class of Service** and select **Class of Service**. On the Search Class of Service page, select the class of service assigned to users in which you want to configure unified messaging. (For information on each field, see **Help> This Page**).

Step 2 On the Edit Class of Service page, in the **Licensed Features** section, check the **Allow Users to Access Voicemail Using an IMAP Client and/ or Single Inbox** check box.

Step 3 You must configure message aging or message quotas. For more information, see the "Message Storage" chapter of the *System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html

Note If you want to permanently delete the messages from Web Inbox, check the **Delete Messages Without Saving to Deleted Items Folder** check box in the **Message Options** section.

Step 4 (*for Text-to-Speech feature only*): In the **Licensed Features** section, check the **Allow Access to Advanced Features** and the **Allow Access to Exchange Email by Using Text to Speech (TTS)** check boxes.

Step 5 Select **Save**.

Unified Messaging Account for Users

Unified Messaging Accounts and User Accounts Related for Unity Connection

Unified messaging accounts connect 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 Users

You can create a large number of unified messaging accounts using Bulk Administration Tool. For information on creating, updating, or deleting unified messaging accounts using BAT tool, see the "Bulk Administration Tool" section of the "Tools" chapter of the *System Administration Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

For information on synchronization behavior if you later disable single inbox in a unified messaging account, see the "Moving and Restoring Exchange Mailboxes" chapter.

Step 1 In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select **Add New** to create a new user or select an applicable user for which you want to create a unified messaging account.

Step 2 Configure unified messaging account (For information on each field, see **Help> This Page**):

a) In the **Edit** menu, select **Unified Messaging Accounts**.
b) On the Unified Messaging Accounts page, select **Add New**.
c) On the New Unified Messaging Accounts page, enter the values of the required fields and select **Save**.

Step 3 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 the mail server, Active Directory, Unity Connection, and the Unity Connection user.

Test Unified Messaging Configuration

View the Summary of Unified Messaging Configuration

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 that 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 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.

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

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging** and select **Unified Messaging Accounts 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 View the following settings:

- To display the Unified Messaging Accounts page for an account, select the icon or the value of the **Alias** column in the applicable row.
- 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 and Unified Messaging with Exchange and 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.

Do the following to check the system configuration and unified messaging configuration:

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

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

Step 3 Select **Refresh** to display links to the latest results.

Step 4 Review the results, resolve problems, if any, and re-run the **Check System Configuration** task until no more problems are found.

Testing Access to Calendars for Unity Connection

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

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 Unity Connection. Select **Send**.

Step 5 Sign in to the Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

Step 6 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 follow the prompts to list meetings. Unity Connection reads the information about the meeting.

Resolving SMTP Domain Name Configuration Issues

When a single inbox user receives a voicemail, it is synchronized from Unity Connection to a mail server. 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 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 Unity Connection address, which may lead to NDR. You must follow the steps further if you want the email address of sender/recipient to be displayed as the corporate email address, for example, userid@corp-hostname, when the voicemail is synchronized for single inbox users from Unity Connection to the mail server.

Do the following procedure to resolve SMTP domain name configuration issues:

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

Step 2 On the Smart Host page, enter the values of the required fields and select **Save** (For information on each field, see **Help> This Page**).

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

Step 3 Configure corporate email address of a user:

a) In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select an applicable user.
b) On the Edit User Basics page, enter value in the **Corporate Email Address** field and select **Save**.

Step 4 In Cisco Unity Connection Administration, expand **System Settings** and select **General Configuration**.

Step 5 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 is sent to the smart host and select **Save**.

Step 6 Configure message action for a user:

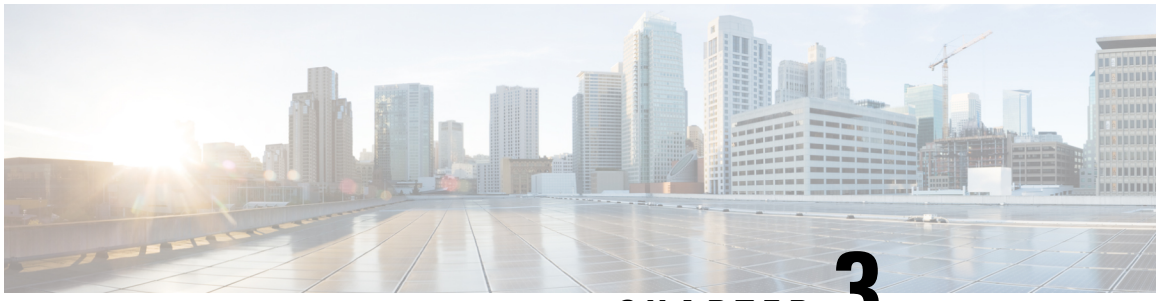
a) In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users Basics page, select an applicable user.
b) On the Edit User Basics page, in the **Edit** menu, select **Message Actions**. On the Edit Message Actions page, select the **Accept the Message** option from the **Voicemail** drop- down list.

Note Make sure to select the **Relay the Message** option from the Email, Fax, and receipt drop -down lists.

Step 7 Setup a recipient policy on the mail server so that the Unity Connection alias resolves to the **Corporate Email Address ID:**

- For Exchange 2019, Exchange 2016 or Exchange 2013, see the following link:

  http://technet.microsoft.com/en-us/library/bb232171.aspx



CHAPTER 3

Configuring Text-to-Speech

Configuring Text-to-Speech

Overview

The Text-to-Speech (TTS) feature allows the unified messaging users to listen to their emails when they sign in to Unity Connection using phone. For more information on text-to-speech, see the Text-to-Speech, Page 1-10 section.

Task List for Configuring Text-to-Speech

With text-to-speech feature enabled in Unity Connection, you can play the emails through phone that are accessible either through Exchange or Office 365.

Configuring the Text-to-Speech Feature

Step 1 Follow the steps depending on the version of Exchange server accessed by unified messaging users:

- Configuring TTS on Office 365, Exchange 2019, Exchange 2016, Exchange 2013 or Exchange 2010.

Step 2 Enable text-to-speech in Unity Connection on an existing or a new unified messaging service. Configure a unified messaging service following the steps as mentioned in the Creating a Unified Messaging Service to Access Mail Server, page 2-27 section.

Note Make sure the Access Exchange Email Using Text-to-Speech (TTS) check box under Service Capabilities is checked.

Configuring TTS on Office 365, Exchange 2019, Exchange 2016, Exchange 2013 or Exchange 2010

Create and install an SSL certificate on each Exchange server that unified messaging users want to access following the given steps:

1. Open the Exchange Management Shell on the Exchange server.
2. Enter the following command:

   new-exchangecertificate -generaterequest -domainname <*Exchange server*> **-friendlyname** <*friendly name*>**-path c:\csr.txt**

   where <*Exchange server*> is the IP address or host name of the Exchange server and <*friendly name*> is the friendly name that you select for the Exchange server

   The domain name for the Exchange server must be the IP address or the fully qualified DNS name (recommended) so that the Unity Connection server can successfully ping the Exchange server. Otherwise, users may not be able to access their emails in the external message store.
3. Press the **Enter** key and a Certificate Signing Request (CSR) file with the name **Csr.txt** is created in the root directory.
4. Send the CSR file to a Certification Authority (CA) that generates and sends back a new certificate.

Note You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange 2019, Exchange 2016, Exchange 2013, or Exchange 2010 server.

5. Enter the following command:

   import-exchangecertificate -path <*path*>

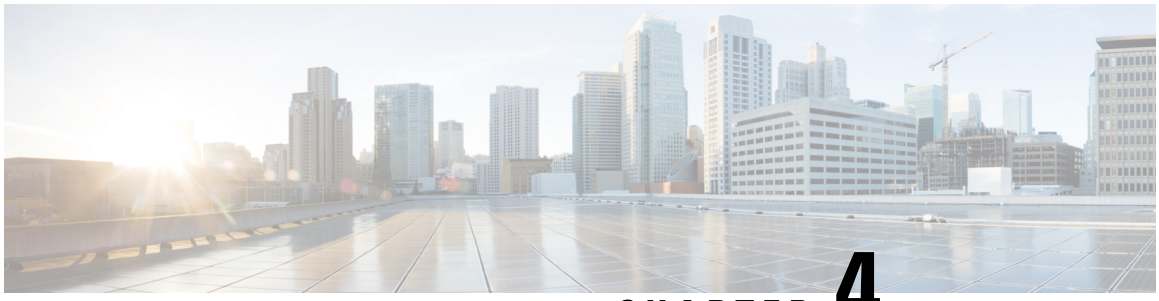
   where <*path*> is the location of the directory where the CA saves the new server certificate
6. Press the **Enter** key and enter the following command:

   dir cert:\localmachine\my | fl
7. Press the **Enter** key and highlight the “thumbprint” property and copy it to the clipboard.
8. Perform either of the following actions:
   - If the class of service for unified messaging users is configured to access email and use calendar data from an external email server using IMAP, enter the following command:

     enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"
   - If the class of service for unified messaging users is not configured to access calendar data from external email server using IMAP, enter the following command:

     enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"
   - Press the **Enter** key.

Note To use TTS over Office 365, you are not required to do any specific configuration.



CHAPTER 4

Configuring Calendar and Contact Integration

Configuring Calendar and Contact Integration

Overview

You can configure calendar and contact integration on Unity Connection with Exchange or Office 365 servers. For more information on calendar and contact integration, see the Calendar and Contact Integration, page 1-11 section.

Configuring Calendar and Contact Integration with Exchange or Office 365 Servers

1. Review the system requirements to ensure that all the requirements for Exchange 2019, Exchange 2016 and Office 365 are met. For more information see the sections "Requirements for Accessing Calendar Information for Meetings" and "Requirements for Accessing Exchange Contact Information" of *System Requirements for Cisco Unity Connection, Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.
2. Configure the Exchange server with which Unity Connection is integrated for calendar and contact integration. See the following sections:
   - Configuring Office 365, Exchange 2019, Exchange 2016, Exchange 2013 or Exchange 2010 for Calendar and Contact Integration
   - Configuring Unity Connection for Calendar and Contact Integration
3. Configure Unity Connection for calendar and contact integration. See the Configuring Unity Connection for Calendar and Contact Integration.
4. *(When enabling Personal Call Transfer Rules only)* Verify that the users or templates are assigned to a class of service that enables them to use the personal call transfer rules feature.
5. Configure the Unity Connection users for calendar and contact integration. See the Configuring Unity Connection Users for Calendar and Contact Integration.

6. Test the calendar integration. See the Testing Calendar Integration with Exchange or Office 365 Servers.

Configuring Office 365, Exchange 2019, Exchange 2016, Exchange 2013 or Exchange 2010 for Calendar and Contact Integration

Do the following tasks to configure Exchange 2019, Exchange 2016, Exchange 2013, Exchange 2010 for the calendar and contact integration:

1. Confirm that **Client Access role** has been enabled on Exchange 2019, Exchange 2016, Exchange 2013 and Exchange 2010 server.
2. Do the Configuring Exchange 2019, Exchange 2016, Exchange 2013, Exchange 2010 for Calendar and Contact Integration.
3. *(Optional)* If you are using SSL for secure access to the Exchange server, follow the steps mentioned in the section Configuring Secure Access to Exchange 2013, Exchange 2010.

Note If you have already configured secure IMAP with SSL on Exchange server and enabled the certificate for both IMAP and IIS, then follow the section Configuring Exchange 2019, Exchange 2016, Exchange 2013, Exchange 2010 for Calendar and Contact Integration.

Configuring Exchange 2019, Exchange 2016, Exchange 2013, Exchange 2010 for Calendar and Contact Integration

Step 1 On the Exchange server, open the **Internet Services (IIS) Manager** application.

Step 2 Go to Internet Information Services > <Exchange server name> > Web Sites > Default Web Site.

Step 3 Right-click Exchange and select **Properties**.

Step 4 In the **Exchange Properties** dialog box, select the **Virtual Directory** tab.

Step 5 From the **Content For This Resource Should Come From** menu, select **A Directory Located On This Computer** .

Step 6 Confirm the Local Path is set to **\\.\BackOfficeStorage\<your-domain.com>\MBX**.

Step 7 Select the **Read** check box.

Step 8 Select the **Directory Security** tab.

Step 9 From the **Authentication and Access Control** menu, select **Edit**.

Step 10 In the **Authenticated Access section of the Authentication Methods** dialog box, check the check boxes for one or more of the following options:

- Integrated Windows authentication (sometimes referred to as NTLM)
- Basic Authentication
- Digest Authentication for Windows Domain Servers

Step 11 Select **OK**.

Step 12 In the **Exchange Properties** dialog box, select **OK**.

Step 13 Go to **Internet Information Services** > **<server name** > **> Web Service Extensions** .

Step 14 In the right-hand pane, select **WebDav** and confirm that the status is "Allowed." If the status is not "Allowed", click **Allow**.

Step 15 On the Exchange server, open the **Exchange Management Console**.

Step 16 Go to **Server Configuration > Mailbox**.

Step 17 Do the following for each mailbox that you want to configure for the calendar and contact integration:

a) In the upper middle pane, select the mailbox name.
b) In the lower middle pane, select the **WebDav** tab.
c) Right-click **Exchange (Default Web Site)** and select **Properties**.
d) In the **Exchange (Default Web Site)** Properties dialog box, select the **Authentication** tab.
e) Select **Use One or More Standard Authentication Methods** and select the same authentication method(s) that you configured in Step 10.

Step 18 Click **OK**.

Step 19 Open the **Exchange Management Shell**.

Step 20 In the **Exchange Management Shell**, enter the following command:

iisbreset /noforce

Step 21 Press **Enter**.

Configuring Secure Access to Exchange 2013, Exchange 2010

Step 1 On the Exchange Server, open the **Exchange Management Shell** application.

Step 2 Enter the following command, where <*Exchange server*> is the IP address or fully qualified domain name of the Exchange server and <*friendly name*> is the friendly name that you selected for the Exchange server:

- **new-exchangecertificate -generaterequest -domainname** <*Exchange server*> **-friendlyname** <*friendly name*>**-path c:\csr.txt**

Caution The domain name for the Exchange server must be the IP address or the fully qualified domain name (recommended) so that the Unity Connection server can successfully ping the Exchange server. Otherwise, the calendar and contact integration may not function correctly.

Step 3 Press **Enter**.

A Certificate Signing Request (CSR) file with the name Csr.txt is created in the root directory.

Step 4 Send the CSR file to a Certification Authority (CA), which generates and sends back a new certificate.

Note You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange server.

Step 5 Save the new certificate in a location that is accessible to the Exchange server on which you want to import the certificate.

Step 6 On the Exchange Server, open the **Exchange Management Shell** application.

Step 7 Enter the following command, where <path> is the full path of the new certificate that you received from the CA:

import-exchangecertificate -path <path>

Step 8 Press **Enter**.

Step 9 Enter the following command:

dir cert:\localmachine\my | fl

Step 10 Press **Enter**.

Step 11 Highlight the “thumbprint” property and press **Ctrl-C** to copy it to the clipboard.

Step 12 If Unity Connection is configured to use IMAP to access both email and calendar data from Exchange server, enter the following command, where <thumbprint> is the “thumbprint” that you copied in Step 11:

enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"

If Unity Connection is not configured to use IMAP but configured to use calendar data from Exchange server, enter the following command, where <thumbprint> is the “thumbprint” that you copied in Step 11:

enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"

Step 13 Press **Enter**.

Step 14 If you want data transmitted as clear text, skip the remaining steps in this procedure and continue with the Configuring Unity Connection for Calendar and Contact Integration. Otherwise, open the **IIS Manager** application.

Step 15 Go to **IIS** > **<server name>** > **Web Sites** > **Default Web Site**.

Step 16 Right-click **Default Web Site** and select **Properties**.

Step 17 In the **Properties** dialog box, select the **Directory Security** tab.

Step 18 From the **Secure Communications** menu, select **Edit**.

Step 19 Check the **Require Secure Channel** check box.

Step 20 Select **OK**.

Step 21 In the **Properties** dialog box, select **OK**.

Configuring Unity Connection for Calendar and Contact Integration

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging** and select **Unified Messaging Services**. You can modify an existing unified messaging service or create a new service using **Add New**.

Step 2 On the New Unified Messaging Service page, in the **Type** list, select **Exchange/BPOS-D** and check the **Enabled** check box to enable the unified messaging service.

Step 3 Enter the details of the required fields and select **Save**. (For information on each field, see **Help> This Page**).

Note Make sure to check the **Access Exchange Calendars and Contacts** check box under **Service Capabilities** menu.

Step 4 Select **Test** and a message appears indicating whether the configuration has been successfully verified. If the verification fails, follow the above configuration steps to ensure that they have been properly implemented.

Configuring Unity Connection Users for Calendar and Contact Integration

After configuring the Unity Connection server for calendar and contact integration, you can configure the applicable users.

Note There must be a user account in Active Directory for each Unity Connection user configured for unified messaging. Also, there must be a corresponding mailbox for each user account in Exchange 2019, Exchange 2016, Exchange 2013, Exchange 2010 that communicates with the Unity Connection server.

Step 1 In Cisco Unity Connection Administration, expand **Users** and select **Users**. Select an applicable user.

Step 2 On the Edit User Basics page, in the **Edit** menu, select **Unified Messaging Accounts**.

Step 3 On the Unified Messaging Accounts page, select **Add New**.

Note Make sure that a unified messaging service is configured before creating unified messaging accounts.

Step 4 On the New Unified Messaging Accounts page, select the following details:

- In **Unified Messaging Service** drop-down, select the unified messaging service created in the sectionConfiguring Unity Connection for Calendar and Contact Integration.
- From the **Account Information** menu, in the **Use This Email Address** field, enter the Exchange email address in Active Directory for the user.

Step 5 In the **Service Capabilities** menu, check the **Access Exchange Calendar and Contacts** check box and select **Save**.

Step 6 Check the calendar and contact configuration for the user, selecting **Test**. The **Task Execution Results** window appears with the test results. If any part of the test fails, verify the configuration for Exchange 2019, Exchange 2016, Exchange 2013, or Exchange 2010, Active Directory, Unity Connection, and the user.

Step 7 Repeat Step 2 through Step 6 for all remaining users.

Testing Calendar Integration with Exchange or Office 365 Servers

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 Unity Connection. Select **Send**.

Step 5 Sign in to the Unity Connection mailbox of the user that you invited to the Outlook meeting:

- 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 2019, 2016, 2013, 2010 meetings.

Configuring Calendar and Contact Integration with Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express

1. Review the system requirements to confirm that all requirements for Cisco Unified MeetingPlace and the Unity Connection server have been met. See the "Requirements for Accessing Calendar Information for Meetings" section of *System Requirements for Cisco Unity Connection Release 14.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.
2. Configure Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express. See the following sections:
   - Configuring Cisco Unified MeetingPlace for Calendar Integration
   - Configuring Cisco Unified MeetingPlace Express for Calendar Integration
3. Configure Unity Connection. See the Configuring Unity Connection for Calendar Integration section.
4. If you configured Cisco Unified MeetingPlace to use HTTPS in step 2., and configured unified messaging services to validate certificates for MeetingPlace servers in step 3.: on the Unity 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 Unity Connection-trust locations. For more information on SSL instructions, see the "Using SSL to Secure Client/Server Connections" chapter of the *Security Guide for Cisco Unity Connection, Release 14.x* , available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html
5. Configure the Unity Connection users. See the Configuring Unity Connection Users for Calendar Integration section.
6. Test the calendar integration. See the Testing Calendar Integration with Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express section.
7. To teach users how to list, join, and schedule meetings, see the "Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 14.x)* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user/guide/phone/b_14cucugphone.html

Configuring Cisco Unified MeetingPlace for 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 are used in the Configuring Unity Connection for Calendar Integration.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace.

Step 7 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 8 Press **Enter**.

Step 9 When prompted to sign in, enter the user ID and password for the privileged service account.

The Cisco Unified MeetingPlace Web Services Description Language (WSDL) download page appears with the title "XFire Services".

Configuring Cisco Unified MeetingPlace Express for Calendar Integration

Step 1 Sign in to Cisco Unified MeetingPlace Express and select **Administration**.

Step 2 Select **User Configuration** > **User Profile Management**.

Step 3 Select **Add New**.

Step 4 Enter the following values in the required fields to create an API user:

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.
Type of User	Select **API User**.

Note The values that you enter for the **User ID, User Password,** and **Profile Number** fields are used in the Configuring Unity Connection Users for Calendar Integration.

Step 5 Select **Save**.

Step 6 Sign out of Cisco Unified MeetingPlace Express.

If you do not sign out of Cisco Unified MeetingPlace Express, the test fails in the Testing Calendar Integration with Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

Step 7 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 Express server):

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

- If SSL is enabled, enter the following URL:

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

Step 8 Press **Enter**.

Step 9 When prompted to sign in, enter the user ID and password for the API user.

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

Configuring Unity Connection for Calendar Integration

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

Step 2 Modify an existing unified messaging service or create a new service by selecting **Add New**.

Step 3 On the New Unified Messaging Service page, in the **Type** list, select **MeetingPlace 8.x** and check the Enabled check box to enable unified messaging with Cisco Unified MeetingPlace server.

Step 4 Enter the values of the required fields and select **Save**. (For information on each field, see **Help> This Page**).

Note Make sure to check the **User MeetingPlace Meetings and MeetingPlace Scheduling and Joining** check boxes under **Service Capabilities** menu.

Step 5 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 Unity Connection.

Configuring Unity Connection Users for Calendar Integration

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

Step 1 In Cisco Unity Connection Administration, expand **Users** and select **Users**. Select an applicable user.

Step 2 On the Edit User Basics page, on the **Edit** menu, select **Unified Messaging Accounts**.

Step 3 On the Unified Messaging Accounts page, select **Add New**. The New Unified Messaging Account page appears.

Step 4 On the New Unified Messaging Account page, select the **Unified Messaging Service** for Cisco Unified MeetingPlace. Enter the values of the required fields and select Save. (For information on each field, see **Help> This Page**).

Note Make sure to check the **MeetingPlace Scheduling and Joining and Primary Meeting Service** check boxes under the **Service Capabilities** menu.

Step 5 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, Unity Connection, and the user.

Step 6 Repeat Step 2 through Step 5 for all remaining users.

Testing Calendar Integration with Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express

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

Step 2 Select **Schedule**.

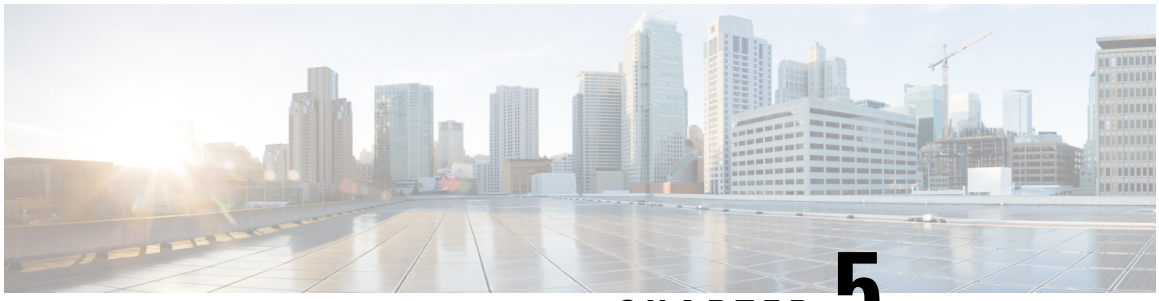
Step 3 Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Unity Connection.

Step 4 Sign in to the Unity 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 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.

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.



CHAPTER 5

Moving and Restoring Exchange Mailboxes

Moving and Restoring Exchange Mailboxes

Overview

The mailboxes for unified messaging users in Cisco Unity Connection can be moved from one Exchange server to another. You may want to move the mailboxes from one Exchange server to another due to any reason. Consider an instance in which after adding the latest supported version of Exchange server to the existing Exchange environment of your organization, you want to move the user mailboxes to the latest version.

To move the user mailboxes from one version of Exchange to another, you need to update some specific settings for the Unity Connection users. This enables Unity Connection to automatically detect the migration of user mailboxes automatically. If Unity Connection fails to detect the migration of mailboxes, you need to manually replace the existing mailboxes of unified messaging users with new mailboxes on the migrated Exchange server.

Updating User Settings After Moving Exchange Mailboxes

As covered in the "Configuring Unified Messaging" chapter, the administrators can create one or more unified messaging services with Exchange. Following are the two settings that identify how Unity Connection manually updates user settings after the Exchange mailboxes are moved:

- Unity Connection searches for Exchange servers: If you select to allow Unity Connection to search for Exchange servers, Unity Connection automatically detects when you move mailboxes to another version of Exchange and automatically updates Unity Connection user settings.
- Unity Connection selects a specific Exchange server: If you select a specific Exchange server, either Unity Connection detects mailbox move from one Exchange server to another or it fails to detect. The administrator needs to manually replace the old unified messaging account with a new unified messaging account to access the specific Exchange server.

Note

- If Unity Connection is not able to automatically detect mailbox moves, see the Replacing Unity Connection Unified Messaging Accounts After Moving Exchange Mailboxes section.
- If Unity Connection automatically detects mailbox moves, see the Moving Exchange Mailboxes to a New Exchange Server section.

Table 5: When Unity Connection Detect Mailbox Moves Between Exchange servers lists the scenarios when Unity Connection can and cannot automatically detect mailbox moves between Exchange servers.

Table 5: When Unity Connection Detect Mailbox Moves Between Exchange servers

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

Moving Exchange Mailboxes to a New Exchange Server

In an organization, you can add an Exchange server by moving the Exchange mailboxes to the new server. If the Exchange mailboxes are associated with Unity Connection users who are configured for single inbox, you must grant the permissions that Unity Connection requires before you move the mailboxes. Otherwise, Unity Connection users cannot access their voicemails from the new location. This is true regardless of whether you allow Unity Connection to search for Exchange servers or you configure Unity Connection to communicate with a specific Exchange server.

For information on granting the necessary permissions depending on the Exchange server, see the Configuring Unified Messaging in Active Directory, page 2-5 section.

Note To access a new Exchange server, either you need to create a new unified messaging services account or grant necessary permissions to the existing unified messaging services account.

Replacing Unity Connection Unified Messaging Accounts After Moving Exchange Mailboxes

Following are the steps the administrators must do when Unity Connection cannot detect Exchange mailbox moves and cannot automatically update the location of the Exchange mailbox for a Unity Connection user:

1. Manually create a new unified messaging account that accesses the new mailbox location.
2. Delete the unified messaging account that accessed the old mailbox location.

Caution Unity Connection does not synchronize voicemails with the corresponding Exchange mailboxes during the time you move the Exchange mailboxes and update Unity Connection settings for the affected users.

Do the following procedure to replace Unity Connection unified messaging accounts after moving exchange mailboxes:

Step 1 Review the Updating User Settings After Moving Exchange Mailboxes to determine whether Unity Connection can automatically detect mailbox moves for your Exchange configuration.

Step 2 Do either of the following steps:

- If Unity Connection can detect mailbox moves, skip the rest of this procedure.
- If Unity Connection cannot detect mailbox moves, continue with Step 3.

Step 3 If you moved the Exchange mailbox to an Exchange server for which there is currently no unified messaging service in Unity Connection, create the service. For more information, see the Creating Unified Messaging Service to Access Mail Server, page 2-27 section.

Step 4 Create a new unified messaging account for the user and select a unified messaging service that accesses the new Exchange server to which the mailbox was moved. For more information, see the Unified Messaging Account for Users, page 2-30 section.

Step 5 Delete the unified messaging account that accessed the old Exchange server from where the mailbox was moved:

a) In Cisco Unity Connection Administration, expand **Users** and select **Users**.
b) On the Search Users page, select the alias of a user.
c) On the Edit User Basics page, from 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. Select **Delete Selected**.

Step 6 Repeat Step 3 through Step 5 for the other users whose Exchange mailboxes you moved.

Restoring Exchange Mailboxes

Restoring exchange mailboxes in Unity Connection requires you to take the backup of the current unified messaging accounts of the users. The following section shows how to restore unified messaging capabilities for individual users or multiple users. The most important aspect while restoring is to disable single inbox to stop the synchronization between Exchange and Unity Connection.

Task List for Restoring Microsoft Exchange Mailboxes

1. Disable single inbox for selected users or for a unified messaging service. See the Disabling Single Inbox for Unity Connection section.
2. Restore Exchange mailboxes. For more information, see the applicable Microsoft documentation.

3. Re-enable single inbox selecting the applicable option:
   - If you disabled single inbox for individual users using Unity Connection\\ Administration, repeat the Disable Single Inbox for Individual Users section, but check the **Synchronize Unity Connection and Exchange Mailboxes (Single Inbox)** check box.
   - If you disabled single inbox for a unified messaging service, repeat the Disable Single Inbox for All Users, 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 using the Bulk Administration Tool, repeat the Disable Single Inbox for a Large Numbers of Selected Users Using the Bulk Administration Tool, but change the value of enableMbxSynch to **1**.

Disabling Single Inbox Before Restoring Exchange Mailboxes

You must disable single inbox for the Unity Connection users whose Exchange mailboxes and other unified messaging service capabilities are being restored. If single inbox is not disabled, Unity Connection is unable to synchronize voicemails received from the time the backup initiates till the restore completes.

Behavior of Synchronization Cache when Single Inbox is Disabled

Unity Connection maintains a synchronization cache that tracks the voicemails already forwarded to Exchange. When you disable single inbox, the synchronization cache is automatically cleared.

Do the following steps to understand the behaviour of synchronization cache when single inbox is disabled:

1. You take the backup of the Exchange server.
2. A new voicemail arrives.
3. Unity Connection synchronizes the voicemail with the Exchange mailbox associated with the Unity Connection user.
4. Unity Connection updates the synchronization cache for the 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 Unity Connection user whose Exchange mailbox was on the failed hard disk.
7. Unity Connection clears the synchronization cache for that user.
8. You replace the hard disk and restore Exchange from the backup that you made in step1.
9. You re-enable single inbox for the user.
10. Unity Connection performs a periodic comparison of the synchronization cache with the voicemails currently in Exchange.
11. Because the cache is empty, Unity Connection concludes that voicemails that are in the Unity Connection mailbox but not in the Exchange mailbox have not yet been synchronized with Exchange.
12. Unity Connection resynchronizes the Unity Connection mailbox with the Exchange mailbox and rebuilds the synchronization cache.

Behavior of Synchronization Cache when Single Inbox is Enabled

If you restore Exchange mailboxes without disabling single inbox for the Unity Connection users, Unity Connection deletes all voicemails received after the backup from which you are restoring. Do the following steps to understand the behaviour of synchronization cache with single inbox:

1. You can take the backup of the Exchange server.
2. A new voicemail arrives.
3. Unity Connection synchronizes the voicemail with the Exchange mailbox associated with the Unity Connection user.
4. Unity Connection updates the synchronization cache for the 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. Unity Connection performs a periodic comparison of the synchronization cache with the voicemails currently in Exchange. The voicemail that arrived in 2. is not in the Exchange mailbox for the associated Unity Connection user.
8. Unity Connection concludes that the voicemail has already been synchronized with Exchange and does not resynchronize the message into the Exchange mailbox.

Disabling Single Inbox for Unity Connection

The first step in restoring Exchange mailboxes is to disable single inbox. Depending on the number of Exchange servers that you are restoring or the effect of restore on Unity Connection functionality, you can disable single inbox in either of the following ways:

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 using Unity Connection\\ Administration. See the Disable Single Inbox for Individual Users.

Restoring Exchange Mailboxes for All the Unified Messaging Users or When Unity Connection Functionality is Not a Concern

You can disable the single inbox functionality of all unified messaging users in either of the following conditions:

- While you are restoring mailboxes for all of the users associated with a unified messaging service.
- While you are restoring mailboxes for selected users associated with a unified messaging service 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 Unity 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 Unity Connection conversation announces that access to messages is unavailable at this time.
- ***Disable the entire unified messaging service:*** If the unified messaging service has other unified messaging features enabled, such as text-to-speech or contact integration, and you disable the service, Unity

Connection conversation stops playing the options for those features until the unified messaging service is re-enabled, which could be confusing for users.

For more information, see the Disable Single Inbox for All Users.

Restoring Exchange Mailboxes for Some Users Associated with a Unified Messaging Service When Unity Connection Functionality is a Concern

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

- 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.

Disable Single Inbox for Individual Users

Step 1 In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select the alias of the user account that you want to modify.

Step 2 On the Edit Users page, in the **Edit** menu, select **Unified Messaging Accounts**. Select the unified messaging account that enables single inbox for the user.

Step 3 Uncheck the **Synchronize Unity Connection and Exchange Mailboxes (Single Inbox)** check box.

Step 4 Select **Save**.

Step 5 Repeat Step 1 through Step 4 for the remaining users.

Disable Single Inbox for All Users

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

Step 1 In Unity Connection Administration, expand **Unified Messaging** and select **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.

Step 3 To disable 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.

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

Step 1 In Cisco Unity Connection Administration, expand **Tools** and select **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 Cisco Unity 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**.

INDEX

C

E

N