



# Messaging

---

- 
- [Overview, on page 1](#)
- [Basics of Messaging, on page 1](#)
- [Integrated Messaging, on page 13](#)
- [Unified Messaging, on page 19](#)

## Overview

This chapter outlines the types of messages available in Cisco Unity Connection, how Unity Connection handles the recording, delivery, storage of messages, and the integrated messaging and unified messaging models.

## Basics of Messaging

Unity Connection handles the recording, playback, storage, and delivery of different types of messages.

## Types of Messages

Following are the different types of messages supported by Unity Connection:

- **Unidentified Voice Messages:** The messages left by outside callers are unidentified or outside caller voice messages. The outside callers are non Unity Connection users or the users who are not signed in to Unity Connection.

An outside caller can call the main phone number for the Unity Connection server and spell by name or enter an extension to reach the user using a handler, or can be directed to the user mailbox (or to a distribution list) through a call handler. If an outside caller calls a user extension and the user does not answer, the call gets forwarded to the voicemail and the caller leaves a voicemail. Unity Connection identifies the senders of these messages as unidentified callers. When an unidentified caller leaves a message, the **From** field of the message displays “UnityConnection@<servername>” in the Web Inbox or in an email client or an RSS reader, if applicable. Depending on whether the subject line has been customized, it displays the phone number of the caller, if it is available. Messages from outside callers can be forwarded to other users but cannot be replied to.

- **User to User Voice Messages:** The messages left by Unity Connection users to another users or distribution lists are identified or user to user voice messages. Users can reply or forward messages from other users.

Consider a user calls another user extension, the called user does not answer and the call is forwarded to user mailbox where the caller leaves a voice message. In this case, if Identified User Messaging is enabled and supported by phone system, and the user calls from primary extension or an alternate device, Unity Connection recognizes that the calling extension is associated with a user or identified user. The identified user messaging is enabled by default. It can be disabled using the Disable Identified User Messaging Systemwide setting on the System Settings > Advanced > Conversations page. Unity Connection does not perform caller authentication or verification when an identified caller leaves a voicemail for another user.

- **Email Messages in Exchange Server:** Users can access emails stored in the user mailboxes on an Exchange server. The Exchange emails can be accessed using the Text-to-Speech feature. For more information, see the [Unified Messaging, on page 19](#) section.
- **System Broadcast Messages:** The recorded announcements sent to everyone in an organization are system broadcast messages. Users must listen to each system broadcast message in its entirety before listening to other new and saved messages or changing setup options. They cannot fast-forward or skip a system broadcast message. For more information, see the [Broadcast Messaging, on page 9](#) section.




---

**Note** By design, system broadcast messages do not trigger message waiting indicators (MWIs) on user phones.

---

- **Text or HTML Notifications:** Message notifications are sent in the form of text messages to email addresses, text pagers, and text-compatible mobile phones. When a new voicemail is delivered to users, they receive SMTP based HTML notifications. For more information, see the [Notifications](#) chapter.
- **Receipts:** A user can request a read receipt when sending a message. The sender receives a message receipt when the recipient listens to the message. New receipts turn on the message waiting indicator on the user phone and can trigger message notifications.

When a voice message cannot be delivered, if the sender is configured to accept receipts, Unity Connection alerts the sender with a nondelivery receipt (NDR). A user can re-send the NDR to a different recipient at a later time. The NDR contains a copy of the original message.

- **Interview Handler Messages:** Interview handlers collect information from callers by playing a series of questions that you have recorded and then recording the answers offered by callers.

When all the answers have been recorded, they are forwarded as a single voice message, with beeps separating the answers, to the recipient (user or distribution list) that you designate in the interview handler configuration.

- **Dispatch Messages:** The dispatch message is sent to a distribution list with the message configured in such a way that only one user responds to that message. A user can accept, decline, or postpone the dispatch message. For more information, see the [Dispatch Messages, on page 3](#) section.
- **Live Record Messages:** The messages recorded during a live conversation between a user and a caller are the live record messages. The recorded messages are stored in the user mailbox. The user can access the messages at any time or forward it another user or group of users. For more information, see the [Live Record, on page 8](#) section.

## Message Recording

The audio format (or codec) used for recording a message is in the same format as used by playback devices. For example, if you listen to messages primarily on a phone system extension, you should configure Unity Connection to record messages in the same audio format that the phone system uses. For more information, see the [Changing the Audio or Video Format of Recordings](#) section.

### Configuring Termination Warning Prompt

By default, Unity Connection plays a termination warning prompt before reaching the maximum allowable message length while callers record their messages. By default, the warning plays 15 seconds before the end of a recording, provided that the recording is not restricted to less than 30 seconds in length.

---

**Step 1** In Cisco Unity Connection Administration, expand System Settings and select Telephony.

**Step 2** On the Telephony Configuration page, enter the values of the following fields:

- Minimum Recording Duration in Milliseconds for Termination Warning
- Recording Termination Warning Time in Milliseconds
- Select Save to apply the changes.

**Note** If the system is temporarily unavailable to take your message, disable the **Recording Termination Warning** by setting the value to zero.

---

## Default Recipient Accounts

The default users are created at the time of installation. The users can be modified but cannot be deleted. Following are the three default users that are responsible for message delivery and retrieval of messages when callers are routed to one of the default call management objects:

- **Operator:** By default, the mailbox of the Operator user stores the messages left for Operator call handler. You should either assign a user to monitor this mailbox or reconfigure the Operator call handler to send messages to a different user or system distribution list.
- **UndeliverableMessagesMailbox:** By default, this mailbox is the only member of the Undeliverable Messages distribution list. You should either assign a user to monitor this mailbox or add a user to the Undeliverable Messages distribution list to monitor and reroute (as appropriate) any messages that are delivered to the list.
- **Unity Connection Messaging System:** By default, this mailbox acts as a surrogate sender for unidentified messages or messages from unidentified callers.

## Dispatch Messages

Dispatch messaging is useful when a team is available to respond to messages and only one member of the team is required to respond.

Following are the ways to handle dispatch messages:

- If a user selects to accept a message, all other copies of the message are removed from the mailboxes of the other members of the distribution list, regardless of whether the other users have listened to or postponed the message.
- If a user selects to postpone the message, it remains as an unread message in the mailbox of that user and in the mailboxes of the other members of the distribution list.
- If the user selects to decline the message, it is removed from the mailbox of that user but copies of the message remain as unread in the mailboxes of the other members of the distribution list.
- If there is only one copy of the dispatch message remaining and no user has yet selected to accept the message, the final user whose mailbox it is in must accept it. That user is not given the option to decline the message.

## Configuring Dispatch Messages

---

- Step 1** In Cisco Unity Connection Administration, expand Call Management and select System Call Handlers.
- Step 2** On the Search Call Handlers page, in the System Call Handlers table, select the applicable call handler.
- Step 3** On the Edit Call Handler Basics page, in the Edit menu, select Message Settings.
- Step 4** On the Edit Message Settings page, under Message Recipient, select a distribution list as the recipient and check the Mark for Dispatch Delivery check box. Select Save.
- 

## Configuring Dispatch Messaging for Interview Handlers

---

- Step 1** In Cisco Unity Connection Administration, expand Call Management and select Interview Handlers.
- Step 2** On the Search Interview Handlers page, in the Interview Handlers table, select the applicable interview handler.
- Step 3** On the Edit Interview Handler Basics page, under Message Recipient, select a distribution list as the recipient and check the Mark for Dispatch Delivery check box. Select Save.
- 

## Dispatch Messaging Limitations and Behavior

Following are the limitations and behavior of dispatch messaging:

- Only voice messages can be flagged for dispatch.
- The handling of dispatch messaging is supported only over the phone interface. If you handle the dispatch messages from any other client interface, such as Web Inbox or Cisco Unified Personal Communicator, the user cannot postpone, accept, or decline the message.




---

**Note** The handling of dispatch messaging is not supported with Visual Voicemail.

---

- The dispatch messages are not synchronized between Unity Connection and Exchange server if single inbox has been configured. For information on single inbox, see the [Unified Messaging, on page 19](#) section.

- The dispatch messages can never be transcribed even if SpeechView has been enabled for the recipients.
- A user can delete the last copy of a dispatch message using Web Inbox or Cisco Unified Personal Communicator.
- During playback of a dispatch message, if a user presses the phone keypad key that is mapped to the “skip” or “delete” menu options, Unity Connection interprets the “skip” key press as “postpone,” and the “delete” key press as “decline.”
- The recipient who accepts the dispatch message is the only user to have a copy of that message in his/her mailbox. The recipient can select to hear the dispatch messages first, during the playback of all voice messages using phone interface.
- The copy of a dispatch message is not stored in the Deleted Items folder if the recipient declines a dispatch message.
- A dispatch message once accepted by a user is treated as a general voice message. Therefore, a dispatch message once accepted cannot be forwarded to another user. The message is presented to the phone interface like a voice message and not announced as a dispatch message.
- If message notification rules are configured for dispatch messages, by the time users receive the notification and call in to retrieve the message, the accepted dispatch messages are gone from the recipient mailboxes.
- The dispatch messaging is not supported for digital networking. For more information on digital networking, see the [Networking](#) chapter.
- For a Unity Connection cluster configuration, two different users can call into the publisher and subscriber servers to accept the same dispatch message if the cluster is stuck in a split brain condition. The split brain condition refers to the time when both publisher and subscriber servers are stuck in Primary state.

After the split brain condition has been resolved, the user who last accepted the dispatch message is the final recipient and the message is removed from the mailbox of the other user.

## Message Delivery

When a message is delivered by Unity Connection, the recipient is either the Unity Connection Messaging system for unidentified messages or the recipient listed in the identified messages.

### Message Delivery and Sensitivity Settings

The message delivery and sensitivity settings allow the users to control the delivery time of a message, the users who can access it, and if the messages can be forwarded to other users.

Following are the message delivery and sensitivity options for users and outside callers:

- **Urgent:** The urgent messages are delivered before other messages. The users who are signed in to the mailboxes can always mark a message urgent.
- **Private:** A private message can be sent to any user but it cannot be forwarded using phone, Messaging Inbox, Web Inbox, ViewMail for Outlook, or ViewMail for Notes. The identified messages can always be marked private and can be saved as .wav files.
- **Secure:** Only Unity Connection users can receive secure messages. The secure messages can be played or forwarded using phone, Messaging Inbox, Web Inbox, or ViewMail for Outlook 8.5. The identified messages can be marked secure but cannot be saved as .wav files.

- Future delivery: A user can mark a message for future delivery to a recipient using the touchtone conversation or the voice recognition conversation. Unity Connection waits to send the message on the day and time that the user specifies. Once future delivery is set on the message, the user can cancel the future delivery as long as the user has not yet selected the option to send the message.

An administrator can cancel the pending messages set for future delivery using the delete cuc futuredelivery CLI command.

The unidentified callers or users who are not signed in to mailboxes, can mark a message urgent, private, or secure depending on the user or user template settings. If any other Unity Connection user calls a user extension and the user does not answer, Unity Connection identifies the caller as unidentified callers. The message delivery and sensitivity settings can be managed in either of the following ways:

- In Cisco Unity Connection Administration> Users> Users> select a user> Edit> Message Settings> select the desirable action under the Message Urgency, Message Security, and Message Sensitivity fields.
- In Cisco Unity Connection Administration> Templates> User Template> select a user template> Edit> Message Settings> select the desirable action under the Message Urgency, Message Security, and Message Sensitivity fields.

## Message Delivery Issues

Following are the information pertaining to message delivery issues:

- If a message failed to be delivered to a recipient that the caller intended to reach, the message is sent to the Undeliverable distribution list. Unity Connection sends a non delivery receipt (NDR) to the sender if the sender is configured to accept NDRs.




---

**Note** NDRs are not send if the sender is an unidentified caller or the mailstore of the recipient is offline.

---

If the original message is malformed, the message is not sent to Undeliverable distribution list. The message is instead sent to the MTA bad mail folder (UmssMtaBadMail).

- If the Unity Connection components involved in message delivery are unavailable, the recorded messages are queued and delivered when the components are available. For example, if a mailbox store is disabled, messages are held in queue, and delivered once the mailbox store is enabled again.

For single inbox configuration, if network or other conditions are slow and prevent attempts to retrieve messages from Exchange, Unity Connection announces to users that email is unavailable. The time period that Unity Connection waits for a response from Exchange is four seconds by default. This can be configured in Cisco Unity Connection Administration> System Settings> Advanced> Unified Messaging Services> the TTS and Calendars: Time to Wait for a Response (in seconds) field.

The messages are held in queue for delivery but they are not synchronized with Exchange mailboxes. The synchronization between Unity Connection and Exchange resumes once Exchange is available.

- If a call is disconnected while users are in the process of sending, replying, or forwarding messages, the messages are handled in the way depending on user configuration. This configuration is specified in either of the following ways:

- In Cisco Unity Connection Administration> Users> Users> select a user> Edit> Send Message Settings> select the desirable action under the When a Call is Disconnected or the User Hangs Up field.
- In Cisco Unity Connection Administration> Templates> User Templates> select a user template> Edit> Send Message Settings> select the desirable action under the When a Call is Disconnected or the User Hangs Up field.
- If the mailbox quota is exceeded or the mailbox store size is exceeded, Unity Connection allows to record the message if the recipient mailbox has not exceeded the Send/ Receive Quota. For more information on mailbox quotas and mailbox store size, see the [Controlling the Size of Mailboxes](#) section of the [Message Storage](#) chapter.

## Message Actions

The message actions for a user or user template determines how to handle the different types of messages received for a user. For more information, see the [Message Actions](#) section.

## Message Subject Line Formats

Message subject lines are visible when users view and listen to messages in the Messaging Inbox, Web Inbox, or any other visual client that displays the message subject. Subject lines are not presented to users when they listen to voice messages by phone. For more information, see the [Subject Line Formats](#) section.

## Message Storage and Disk Capacity

The message content is stored as .wav file on the Unity Connection server and the information about the messages is stored in a database.

## Message Deletion

The users can delete messages using multiple methods, such as phone, Web Inbox, or Messaging Inbox. In addition to this, an administrator can also manage the message deletion to meet the disk capacity requirements and security needs.

Following are the ways to delete messages:

- The messages can be either soft deleted or hard deleted depending on the settings configured in Cisco Unity Connection Administration> Class of Service> class of service for the users> the Delete Messages without Saving to Deleted Items Folder check box under the Message Options field.

If the check box is unchecked and a user deletes a message, then the deleted message moves to the Deleted Items folder. This action is referred to as soft delete.

If the check box is checked and a user deletes a message, then the message is permanently deleted without sending any copy to Deleted Items folder. This action is referred to as hard delete.

- The messages can be permanently deleted without any action required from the users who received them, using the message aging policies. For more information, see the [Message Aging Policies](#) section.

- The messages can be deleted using the Message File Shredding Level setting in the Messaging Configuration page in Cisco Unity Connection Administration > Advanced System Settings. This is a system wide setting that ensures copies of messages are securely deleted by shredding the messages the specified number of times when they are deleted. The shredding can be done only when they have been hard deleted.

## Message Access

Users can access new and saved voice messages using a touchtone or voice recognition conversation over phone. You can specify whether users can access the deleted messages.

The users may also gain access to voice messages using Web Inbox, Messaging Inbox, Cisco Unified Personal Communicator, RSS reader or other applications. For information on accessing voice messages using RSS reader, see the [Enabling Insecure RSS Connections](#) section.

Depending on the unified messaging service accounts, users may access email messages in an external message store using phone.

## Live Record

Live record allows users to record conversations while they talk to callers. The recorded conversation is stored as a message in the user mailbox and the user can review it later, or redirect it to another user or group of users. Operators in your organization may find live record particularly useful. Live record is supported only for Cisco Unified Communications Manager integrations.

The live record does not work for users who have full mailboxes. When a user with a full mailbox tries to record a call, the recorded conversation is not stored as a message in the user mailbox.

## Configuring Live Record

**Step 1** Add a live record pilot number to Cisco Unified Communications Manager:

- In Cisco Unified Communications Manager Administration, expand Call Routing and select Directory Number.
- In the Find and List Directory Numbers page, select Add New. The Directory Number Configuration page appears.
- In the Directory Number field, enter the directory number of the live record pilot number.
- In the Route Partition field, select the partition that contains voicemail port directory numbers.
- In the Description field, enter a description.
- In the Voice Mail Profile field, accept the default of None.
- In the Calling Search Space field, select the calling search space that includes the partition with all voicemail port directory numbers.
- In the Forward All field, under Destination, enter the voicemail pilot number for the voice messaging ports.
- In the Forward All field, under Calling Search Space, select the calling search space that includes the partition with all voicemail port directory numbers and select Save.

**Step 2** (optional) Configure Cisco Unified Communications Manager conference settings:

- In Cisco Unified Communications Manager Administration, expand System and select Service Parameters.
- On the Service Parameters Configuration page, in the Server field, select the name of the Cisco Unified CM server.
- In the Service list, select Cisco CallManager. In the Clusterwide Parameters (Feature - Conference), in the Drop Ad Hoc Conference field, select When Conference Controller Leaves and select Save.



**Step 3** Create a routing rule for live record in Unity Connection:

- a) In Cisco Unity Connection Administration, expand Call Management and select Call Routing > Forwarded Routing Rules.
- b) On the Forwarded Routing Rules page, select Add New.
- c) On the New Forwarded Routing Rule page, enter a description in the Description field and select Save.
- d) On the Edit Forwarded Routing Rule page, in the Status field, select Active.
- e) In the Send Call To field, select Conversation.
- f) In the Conversation list, select Start Live Record and select Save.
- g) In the Routing Rule Condition section, select Add New.
- h) In the New Forwarded Routing Rule Condition page, select Forwarding Station. To the right of the Forwarding Station option, select Equals and enter the live record pilot number that you created in the To Add a Live Record Pilot Number to Cisco Unified CM field and select Save.

**Step 4** (optional) Adjust the live record beep interval:

- a) In Cisco Unity Connection Administration, expand System Settings and select Advanced > Telephony.
- b) In the Telephony Configuration page, enter value in the Live Record Beep Interval in Milliseconds field. (For more information on this field, see Help> This Page).
- c) Select Save.

**Step 5** Test the live record:

- a) From a user phone, dial an extension.
- b) After the dialed extension is answered, on the user phone, press the Confm softkey to start a conference call.
- c) Dial the live record pilot number that you created in Cisco Unified Communications Manager.
- d) Press the Confm softkey to join the Unity Connection live recorder with the conference call.
- e) After recording the phone conversation, hang up the user phone. Sign in to the voice mailbox for the user and listen to the recorded phone conversation.

---

## Broadcast Messaging

System broadcast messages are different from regular voice messages in the following ways:

- The users when sign in to Unity Connection using phone, immediately hear the number of broadcast messages they have and the system begins playing them. This happens even before users hear message counts for new and saved messages.
- The sender of a broadcast message specifies the time for which the message is active. The system can broadcast the message till it is active. The message can be active for a day, week, month or for an indefinite time period.
- The playback of a broadcast message can be interrupted by a user, for example, a user hangs up. The message plays again the next time when the user signs in to Unity Connection using phone.
- The broadcast message can either be replayed or permanently deleted after a user has finished playing a system broadcast message. Users cannot respond to, forward, or save broadcast messages.
- The users can receive an unlimited number of system broadcast messages even when they exceed the mailbox size limits and are no longer able to receive other messages. This is because the storage of broadcast messages is not included in the total mailbox size for each user.

- The users can listen to broadcast messages only using phone. Other clients, such as RSS reader and Web Inbox cannot be used to listen to broadcast messages.
- The single inbox messages are not synchronized between Unity Connection and Exchange server.
- Unity Connection stops responding to voice commands during the playback of voice messages. When using the voice-recognition input style, users need to use key presses to either replay or delete the broadcast message.

Follow the given steps to configure broadcast messaging to users:

1. Set up a way for users to access the Broadcast Message Administrator. See the [Enable Phone Access to the Broadcast Message Administrator](#) section.
2. Enable user accounts or a template to send and update system broadcast messages. See the [Enabling Sending and Updating Broadcast Messages](#) section.

## Enable Phone Access to the Broadcast Message Administrator

To send a system broadcast message, users sign in to the Broadcast Message Administrator, a special conversation that allows them to send and update system broadcast messages. You can give users access to the Broadcast Message Administrator using either of the following ways:

- Configure a Custom Keypad Mapping conversation: The Custom Keypad Mapping tool can be configured to map a key to the Broadcast Message Administrator Conversation so that it is offered to users from the main menu. See the [Custom Keypad Mapping Tool](#) section.
- Create a call handler: See the [Creating a Call Handler to Send Users to the Broadcast Message Administrator, on page 10](#) section.
- Set up a one-key dialing option: See the [Setting Up a One Key Dialing Option to Send Users to Broadcast Message Administrator, on page 11](#) section.
- Set up a phone number and routing rule: Set up a new phone number and then add a routing rule. See the [Setting Up a Routing Rule to Send Users to Broadcast Message Administrator, on page 11](#) section.

### Creating a Call Handler to Send Users to the Broadcast Message Administrator

A new call handler with unique extension is created to specify the Broadcast Message Administrator as the destination to which Unity Connection sends the user after hearing the greeting.

- 
- Step 1** In Cisco Unity Connection Administration, expand Call Management and select System Call Handlers.
- Step 2** In the Search Call Handlers page, select Add New.
- Step 3** In the New Call Handler page, enter a display name and the extension that users can dial to reach the call handler. Select the call handler template on which to base the new call handler and select Save.
- Step 4** In the Edit Call Handler Basics page, in the Edit menu, select Greetings.
- Step 5** In the Greetings page, select the Standard greeting.
- Step 6** In the Edit Greeting page, in the Callers Hear section, select Nothing.
- Step 7** In the After Greeting section, select Conversation and then select Broadcast Message Administrator and select Save.
-

## Setting Up a One Key Dialing Option to Send Users to Broadcast Message Administrator

You can specify that Unity Connection sends a caller to the Broadcast Message Administrator when a caller presses a particular key during the greeting. To set up a one-key dialing option for accessing the Broadcast Message Administrator, use either of the following procedures:

- 
- Step 1** In Cisco Unity Connection Administration, expand Call Management and select System Call Handlers.
  - Step 2** In the Search Call Handlers page, select the applicable call handler. If you want to set up access to the Broadcast Message Administrator from the opening greeting, select the Opening Greeting call handler.
  - Step 3** In the Edit Call Handler Basics page, in the Edit menu, select Caller Input.
  - Step 4** In the Caller Input page, in the Caller Input Keys table, select the applicable phone keypad key.
  - Step 5** In the Edit Caller Input page for the key that you have selected, check the Ignore Additional Input (Locked) check box.
  - Step 6** In the Conversation section, select Broadcast Message Administrator and then select Save.
- 

## Setting Up a One Key Dialing Option from a User Greeting to Access Broadcast Message Administrator

- 
- Step 1** In Cisco Unity Connection Administration, expand Users and select Users.
  - Step 2** In the Search Users page, in the Search Results table, select the applicable user.
  - Step 3** In the Edit User Basics page, in the Edit menu, select Caller Input.
  - Step 4** In the Caller Input page, in the Caller Input Keys table, select the applicable phone keypad key.
  - Step 5** In the Edit Caller Input page for the key that you have selected, check the Ignore Additional Input (Locked) check box.
  - Step 6** In the Conversation section, select Broadcast Message Administrator and then select Save.
- 

## Setting Up a Routing Rule to Send Users to Broadcast Message Administrator

- 
- Step 1** In Cisco Unity Connection Administration, expand Call Management > Call Routing and select Direct Routing Rules.
  - Step 2** In the Direct Routing Rules page, select Add New.
  - Step 3** In the New Direct Routing Rule page, enter a display name for the new routing rule and select Save.
  - Step 4** In the Edit Direct Routing Rule page, confirm that the Status is set to Active.
  - Step 5** In the Send Call To field, in the Conversation section, select Broadcast Message Administrator and select Save.
  - Step 6** In the Routing Rule Conditions table, select Add New.
  - Step 7** In the New Direct Routing Rule Condition page, in the Dialed Number section, select Equals and enter the phone number that has been set up for access to the Broadcast Message Administrator. Select Save.
  - Step 8** In the Direct Routing Rule menu, select Direct Routing Rules. Make sure that the new routing rule is in an appropriate position in the routing table.
  - Step 9** (optional) If you want to change the order of routing rules, select Change Order. In the Edit Direct Routing Rule Order page, select the name of the rule you want to reorder, and select the Up or Down arrow until the rules appear in the correct order. Select Save.
-

## Enabling Sending and Updating Broadcast Messages

After configuring the Broadcast Message Administrator, you need to enable users to send or update broadcast messages using either of the following ways:

- 
- Step 1** In Cisco Unity Connection Administration, expand Users and select Users.
  - Step 2** In the Search Users page, select the applicable user. For more than one user, check the check boxes against the applicable users and select Bulk Edit.
  - Step 3** In the Edit User Basics page, in the Edit menu, select Send Message Settings.
  - Step 4** In the Send Message Settings page, under Broadcast Messages, check the applicable check boxes and select Save. (For more information on each field, see [Help > This Page](#)).
- 

### Enabling Sending and Updating Broadcast Messages for User Templates

- 
- Step 1** In Cisco Unity Connection Administration, expand Templates and select User Templates.
  - Step 2** In the Search User Templates page, select the applicable user template. For more than one user template, check the check boxes against the applicable user templates and select Bulk Edit.
  - Step 3** In the Edit User Template Basics page, in the Edit menu, select Send Message Settings.
  - Step 4** In the Send Message Settings page, under Broadcast Messages, check the applicable check boxes and select Save. (For more information on each field, see [Help > This Page](#)).
- 

## Importance of Broadcast Message Administrator

The users allowed to send and update broadcast messages can use the Broadcast Message Administrator to do the following tasks:

- Record and send one or more broadcast messages.
- Define when a system broadcast message becomes active and for how long. The date and time reflect the time zone for the user who sends the message.




---

**Note** If a sender hangs up or is disconnected while creating a broadcast message but before sending it, Unity Connection deletes the recording.

---

The users allowed to update broadcast messages can use the Broadcast Message Administrator to do the following tasks:

- Review active messages. If there is more than one active message, the Broadcast Message Administrator presents them in order based on the start date and time, starting with the newest messages.
- Change the end date and time for active messages.
- Change or add to a recording for future messages.

- Change the start date and time or the end date and time for future messages. (Note that the end date and time does not adjust automatically if senders change the start date and time but do not change the end date and time.)
- Delete active and future messages.

## Changing Broadcast Message Administrator Defaults

Default behavior for the Broadcast Message Administrator is controlled by settings on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration.

Following are the changes you can make to the system defaults:

- **Retention Period:** This indicates the time for which Unity Connection retains the expired broadcast messages on the server. By default, the .WAV file and any data associated with a message purges in 30 days. To change the retention period for expired broadcast messages, enter a number from one to 60 days.
- **Default Active Days:** This indicates the number of days that a broadcast message remains active when the sender does not specify an end date and time. The default is 30 days. To change how long a message without an end date and time remains active, enter a number from zero (0) to 365 days. A value of zero (0) days means that messages that are sent without a specified end date and time remain active indefinitely.
- **Maximum Recording Length:** This indicates the maximum length allowed for system broadcast messages. By default, senders can record messages up to 300,000 milliseconds (5 minutes) in length. To change the maximum recording length, enter a number from 60,000 (1 minute) to 36,000,000 (60 minutes) milliseconds.
- **Play Oldest Message First:** This indicates the order in which broadcast messages are presented to users. By default, the check box is checked that plays the oldest message first. To play the newest message first, uncheck the check box.

## Integrated Messaging

The model of messaging in which there are separate user accounts handle the voicemails and emails for a user is known as integrated messaging. The emails for a user are managed through the user mailbox on an email server and the voicemails for a user are managed through a user mailbox in Unity Connection.

Unity Connection supports IMAP and SMTP protocols for integrated messaging. The SMTP protocol is used for sending messages to another users and IMAP protocol is used for retrieval of messages.

## SMTP Message Handling

Unity Connection can receive and process SMTP messages generated by IMAP clients, for example, a voice message recorded in a Microsoft Outlook email client using ViewMail for Outlook.

When an authorized IMAP client tries to send a message to Unity Connection through SMTP, the message is categorized as a voicemail, email, fax, or delivery receipt. The sender is mapped to a user and the message recipients are mapped to users or contacts by comparing the SMTP address in the message header to its list of SMTP proxy addresses.

Unity Connection processes the message for each recipient under either of the given conditions:

- If SMTP authentication is configured for IMAP client and SMTP address of the sender matches a proxy address or primary SMTP address for the authenticated user.
- If SMTP authentication is not configured for the IMAP client and the SMTP address of the sender matches a proxy address or primary SMTP address for any Unity Connection user.

Following are the types of recipient based on which Unity Connection processes the messages for each individual:

- If the recipient maps to a VPIM contact, Unity Connection converts the message into a VPIM message, removing any attachment that is not allowed by the VPIM standard. Unity Connection either delivers the message to the specified VPIM location if the VPIM location is homed on the local server, or forwards it to another digitally networked Unity Connection server for delivery if the VPIM location is homed on that server. For more information on VPIM, see the Networking Guide for Cisco Unity Connection, Release 15, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/networking/guide/b\\_15cucnetx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/networking/guide/b_15cucnetx.html).
- If the recipient maps to a user homed on the local server, Unity Connection performs the action specified on the Message Actions page of the profile for the user in Cisco Unity Connection Administration. For each type of message (voice, email, fax, or delivery receipt) you can configure whether the message is accepted and placed in the user mailbox on the Unity Connection server, relays the message to the user at an alternate SMTP address, or rejects the message and generates a non delivery receipt (NDR).
- If the recipient maps to a user homed on a remote Unity Connection server, the message is relayed to the home server of the user that performs the action specified on the Message Actions page of the user profile.
- If the recipient does not map to any of the above, Unity Connection either relays the message to the SMTP smart host or sends an NDR to the sender, depending on the option selected for the When a Recipient Cannot be Found setting on the System Settings > General Configuration page in Cisco Unity Connection Administration. By default, Unity Connection sends an NDR.

If SMTP authentication is configured for the IMAP client and the SMTP address of the sender does not match a proxy address or the primary SMTP address for the authenticated user, the Unity Connection server returns an SMTP error that causes the message to remain in the client outbox.

If SMTP authentication is not configured for the IMAP client and the SMTP address of the sender does not match any known user proxy address or primary SMTP address, Unity Connection places the message into the MTA bad mail folder (UmssMtaBadMail).

## Example Using IMAP and ViewMail for Outlook

Consider an example of an organization ExampleCo. that uses Microsoft Outlook to access a Microsoft Exchange server for email. Each employee at the company receives corporate email at an address that follows the pattern <firstname.lastname@example.com>. ExampleCo wants employees to be able to use Outlook to access voice messages stored on the Unity Connection server. To allow employees to send, forward, or reply to voice messages in the Outlook client, ExampleCo deploys the Cisco Unity Connection ViewMail for Microsoft Outlook plugin. The Outlook client for each employee is configured to access the user account using IMAP.

When Robin Smith at ExampleCo wants to send an email message to a coworker, Chris Jones, Robin composes a new email message to [chris.jones@example.com](mailto:chris.jones@example.com). By default, Outlook is configured to route new email messages to the Microsoft Exchange server for delivery. Next, Robin wants to send Chris a voice message and selects the New Voice Message icon that opens the ViewMail for Outlook form. Robin again addresses

the message to `chris.jones@example.com`, records audio for the message, and selects the Send button. The voice message is routed to Unity Connection for delivery because ViewMail is configured to use Unity Connection IMAP accounts to send the messages.

When Unity Connection receives the voice message, it searches the list of SMTP proxy addresses for `robin.smith@example.com` (the sender) and `chris.jones@example.com` (the recipient). Unity Connection delivers the message as a voice message from Robin Smith to Chris Jones because these addresses are defined as SMTP proxy addresses for the user profiles of Robin Smith and Chris Jones respectively.

When Chris opens Outlook, the email message from Robin shows up as a new message in the Microsoft Exchange Inbox. The voice message from Robin, on the other hand, shows up as a new message in the Inbox of the Unity Connection account that Chris accesses using IMAP. If Chris replies to either message, the Outlook client automatically route the reply using the account in which Chris received the original message.

## Important Points for Deploying Integrated Messaging

Following are the considerations when deploying IMAP clients to send and receive Unity Connection messages:

- Use a firewall to protect the SMTP port from unauthorized access. The SMTP port and domain are listed on the System Settings > SMTP Configuration > Server page in Cisco Unity Connection Administration.
- Configure Transport Layer Security for IMAP client connections in order to protect user passwords.
- Configure the corporate email address of each user as an SMTP proxy address for the user. When setting up the Unity Connection IMAP account on user workstation, use the corporate email address of the user instead of the Unity Connection specific email address. In this way, users are insulated from changes to the Unity Connection-specific addresses if the SMTP domain is changed.
- Create a separate Outlook address book for ViewMail users that is limited to the objects in the user search space if you are using search spaces to limit the objects that users can reach and do not want users to receive NDRs for unreachable objects.

## Task List for Configuring IMAP Access

Follow the given steps to configure IMAP access to Unity Connection messages:

1. (optional) Do the following tasks if you plan to configure Unity Connection to relay messages for users to another SMTP server:
  - Configure the SMTP smart host to accept messages from Unity Connection server. For more information, see the documentation for the SMTP server you are using.
  - Configure Unity Connection to relay messages to smart host. For more information, see the [Configuring Unity Connection to Relay Messages to a Smart Host](#) section.
  - Review the settings that control whether private or secure messages can be relayed. For more information, see the [Configuring Message Relay Settings](#) section.
2. Configure message actions for users or user templates. For more information, see the [Configuring Message Actions for Users or User Templates](#) section.
3. Configure SMTP proxy addresses for users who send or receive messages from IMAP clients. For more information, see the [Configuring SMTP Proxy Addresses for Users or User Templates](#) section.

4. Associate users with a class of service that offers a license to use an IMAP client to access voice messages. For more information, see the [Enabling IMAP Client Access to Voice Messages for Users](#) section.
5. Configure SMTP proxy addresses for VPIM contacts who may receive messages from IMAP clients. For more information, see the [Configuring SMTP Proxy Addresses for Contacts](#) section.
6. If you configured Transport Layer Security to be required or optional in the procedure in Task 7.: Configure the Unity Connection server to provide a secure IMAP Unity Connection, as described in the “Securing Cisco Unity Connection Administration, Cisco PCA, Cisco Unity Connection SRSV, and IMAP Email Client Access to Cisco Unity Connection” section in the “Using SSL to Secure Client/ Server Connections in Cisco Unity Connection” chapter of the *Security Guide for Cisco Unity Connection, Release 15*, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/security/b\\_15cusecx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/b_15cusecx.html).
7. Configure Unity Connection to allow SMTP connections from IMAP clients. For more information, see the [Configuring IMAP Client Access and Authentication](#) section.
8. (optional) If you want to customize SMTP settings, do the steps as mentioned in the [Configuring SMTP Message Parameters](#) section.
9. Configure a supported IMAP client to access the SMTP messages in the user mailbox. For more information, see the “Configuring an Email Account to Access Cisco Unity Connection Voice Messages” chapter of the *User Workstation Setup Guide for Cisco Unity Connection, Release 15* available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/user\\_setup/guide/b\\_15cucuwx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/user_setup/guide/b_15cucuwx.html).

## Configuring Unity Connection to Relay Messages to a Smart Host

---

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

**Step 2** In the Smart Host page, in the Smart Host field, enter the IP address or fully qualified domain name of the SMTP smart host server and select Save. (For more information on each field, see Help> This Page).

**Note** The Smart Host can contain up to 50 characters.

---

## Configuring Message Relay Settings

---

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

**Step 2** Configure message relay settings (For information on each field, see Help> This Page):

- a) To mark the relay messages private, check the Allow Relaying of Private Messages check box.
- b) To mark the relay messages secure, check the Allow Relaying of Secure Messages check box and select Save.

**Note** Unity Connection sends an NDR to the message sender when it receives a message that it cannot relay because the message is marked private or secure.

---



## Configuring Message Actions for Users or User Templates

---

- Step 1** In Cisco Unity Connection Administration, expand Users> Users and select the applicable user. To apply changes in user template, expand Templates> User Templates and select the applicable user template.
  - Step 2** In the Edit menu of the user or user template, select Message Actions.
  - Step 3** In the Edit Message Actions page, enter the values of the required fields and select Save. (For information on each field, see Help> This Page).
- 

## Configuring SMTP Proxy Addresses for Users or User Templates

---

- Step 1** In Cisco Unity Connection Administration, expand Users> Users and select the applicable user. To apply changes in user template, expand Templates> User Templates and select the applicable user template.
  - Step 2** In the Edit menu of the user or user template, select SMTP Proxy Addresses.
  - Step 3** In the SMTP Proxy Addresses page, select Add New to add a new SMTP proxy address. Enter the values of the required fields and select Save. (For information on each field, see Help> This Page).
- 

## Enabling IMAP Client Access to Voice Messages for Users

---

- Step 1** In Cisco Unity Connection Administration, expand Class of Service and select Class of Service. The Search Class of Service page appears displaying the currently configured class of services.
  - Step 2** Select the class of service that you want to update. If you select more than one class of service, select Bulk Edit.
  - Step 3** On the Edit Class of Service page, under Licensed Features, select the Allow Users to Access Voicemail Using an IMAP Client and/ or Single Inbox field. Check the applicable check boxes. (For more information on each field, see Help> This Page).
  - Step 4** Select Save.
- 

## Configuring SMTP Proxy Addresses for Contacts

---

- Step 1** In Cisco Unity Connection Administration, expand Contacts and select Contacts. Select the contact that you want to update. If you select more than one contact, select Bulk Edit.
  - Step 2** On the Edit Contact Basics page, in the Edit menu, select SMTP Proxy Addresses.
  - Step 3** On the SMTP Proxy Addresses page, select Add New to add an SMTP proxy address. Enter the address and select Save.
- 

## Configuring IMAP Client Access and Authentication

---

- Step 1** In Cisco Unity Connection Administration, expand System Settings > SMTP Configuration, then select Server. The SMTP Server Configuration page appears.

- Step 2** Configure IP address access list (For more information, see [Help > This Page](#)):
- In the Edit menu, select Search IP Address Access List.
  - In the Search IP Address Access List page, select Add New to add a new IP address to the list.
  - In the New Access IP Address page, enter an IP address and select Save.
  - In the Access IP Address page, to allow connections from the IP address, check the Allow Unity Connection check box and select Save.

---

## Configuring SMTP Message Parameters

You can configure Unity Connection to reject any incoming SMTP messages that are larger than a configurable total size or have more than a configurable number of recipients.

- Step 1** In Cisco Unity Connection Administration, expand System Settings > SMTP Configuration and select Server.
- Step 2** In the SMTP Server Configuration page, in the Limit Size of Message field, enter a number in kilobytes to limit the size of an individual message sent by an SMTP client.
- Step 3** In the Limit Number of Recipients per Message field, enter the number of recipients allowed per message and select Save.

---

## Configure SMTP client communication

### Over STARTTLS on Port 25

Unity Connection Release 14SU1 and earlier, supports secure SMTP client communication. You can configure Unity Connection to support secure SMTP client interface using STARTTLS.

- Step 1** To enable Secure SMTP client feature, execute
- ```
run cuc dbquery unitydirdb update tbl_configuration set valuebool='1'
where name ='SmtpSecureClientEnabled'
```
- CLI command. By default this feature is disabled.
- Step 2** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration** and select **Server**.
- Step 3** (Applicable to both Server and Client side configuration) On **SMTP Server Configuration** page check option **Allow Connections From Untrusted IP Addresses**. Make sure the value of field **Transport Layer Security From Untrusted IP Addresses** is same on client and SMTP Smart Host.
- Note** Cisco Unity Connection and SMTP client communication will be at port 25 using STARTTLS.
- Step 4** Select Save to apply the changes.

---

### Over STARTTLS on Port 25 and 587 using Authentication Support

Unity Connection Release 14SU2 and later, supports secure SMTP client communication over port 25 and 587 using Authentication support. You can configure Unity Connection to support secure SMTP client interface using STARTTLS on port 587. You can also authenticate SMTP client interface using username and password.

**Step 1**

Server side configuration:

- a) In Cisco Unity Connection Administration, expand **System Settings> SMTP Configuration** and select **Server**.
- b) You can choose SMTP Port that Unity Connection uses for incoming and outgoing SMTP connections between 25 and 587.
- c) Select other fields on SMTP Server Configuration page as per requirement.
- d) Select Save to apply the changes. (For more information on each field, see **Help> This Page**).
- e) For changes to take effect, you must restart the Connection SMTP Server service in Cisco Unity Connection Serviceability. If a Connection cluster is configured, restart the service on both nodes.

**Step 2**

Client side configuration:

- a) In Cisco Unity Connection Administration, expand **System Settings> SMTP Configuration** and select **Smart Host**.
- b) To enable Secure SMTP client feature, check option **Enable Secure Client**.
- c) You can choose secure port between 25 and 587 using **Host Port** field if **Enable Secure Client** option is checked.
- d) To enable authentication support, check the **Use Authentication** option and enter the details of password protected Smart Host. You must enter username and password if this option is checked.
- e) Select Save to apply the changes. (For more information on each field, see **Help> This Page**).
- f) For changes to take effect, you must restart the Connection SMTP Server service in Cisco Unity Connection Serviceability. If a Connection cluster is configured, restart the service on both nodes.

## Unified Messaging

The model of messaging in which different types of messages are integrated into a single interface and accessible from variety of devices is known as unified messaging. The voicemails, emails, and faxes are all stored in a single message store, for example, an Exchange mailbox store. The voice messages in the supported mail servers are synchronized with the user mailbox in Unity Connection.

Unity Connection is supported to be integrated with the following servers:

- Microsoft Exchange 2019, 2016.
- Microsoft Office 365
- Gmail Server.

The unified messaging, also known as the single inbox feature also supports access to Exchange calendars and contacts, transcription of voice messages, notification of upcoming meeting over phone, and many other features. For more information on configuring unified messaging and the supported features, see the *Unified Messaging Guide for Cisco Unity Connection, Release 15* available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/unified\\_messaging/guide/b\\_15cucumgx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/unified_messaging/guide/b_15cucumgx.html).

## Cisco Voicemail for Gmail

Unity Connection 15 and later provides a new way to users for accessing the voicemails on their Gmail account. For this, you need to configure unified messaging with **Google Workspace** to synchronize the voicemails between Unity Connection and Gmail server.

**Cisco Voicemail for Gmail** provides a visual interface for an enriched experience with voicemails at Gmail. With this extension, user can perform the following :

- Compose a voicemail from within Gmail.
- Play the received voicemail without the need of any external player.
- Compose a voicemail in reply-to a received message.
- Compose a voicemail while forwarding a received message.

Follow below steps for using chrome extension:

1. Administrator should configure Unified Messaging with Google Workspace using steps mentioned in [Task List for Configuring Unified Messaging with Google Workspace](#) section of the "Configuring Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release 15* available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/unified\\_messaging/guide/b\\_15cucumgx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/unified_messaging/guide/b_15cucumgx.html).
2. Administrator should add SMTP proxy addresses for Unified Messaging users in Unity Connection by following below steps:
  - Login **Cisco Unity Connection Administration**.
  - On the **Edit Users Basics** page, enter user's Gmail ID in **Corporate Email Address** field.
  - Enable **Generate SMTP Proxy Address From Corporate Email Address** checkbox corresponding to user.
3. Users can now configure and use the chrome extension. For more information, see the *Quick Start Guide for Cisco Voicemail for Gmail* available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/vmg/quick\\_start/guide/b\\_cucqsvmgchrext.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/vmg/quick_start/guide/b_cucqsvmgchrext.html).



---

**Note** Steps to configure Cisco Voicemail for Gmail chrome extension cannot be performed in bulk by Administrator.

---