Securing User Messages in Cisco Unity Connection

By setting message sensitivity, users can control who can access a voice message and whether it can be redistributed to others. Cisco Unity Connection also offers ways for you to prevent users from saving voice messages as WAV files to their hard drives or other locations outside the Unity Connection server, enabling you to maintain control of how long messages are retained before they are archived or purged. Unity Connection also offers methods for managing the secure deletion of messages.

See the following sections:

How Cisco Unity Connection Handles Messages That Are Marked Private or Secure

When users send messages by phone in Cisco Unity Connection, the messages can be marked private, secure, or both private and secure. You can also specify whether Unity Connection marks messages that are left by outside callers as private, secure, or both.

Private Messages

-
- A private message can be forwarded and can be saved locally as a WAV file when accessed from an IMAP client unless you specify otherwise. (See the "Message Security Options for IMAP Client Access in Cisco Unity Connection" section on page 11-5 to learn how to prohibit users from playing and forwarding private messages and from saving private messages as WAV files.)
- When users reply to a private message, the reply is marked private.
- When users send a message, they can choose to mark it private.
- When outside callers leave a message, they can choose to mark it private if the system is configured with message delivery and sensitivity option for private messages
- When users do not explicitly sign in to their mailboxes before leaving messages for other users, they can choose to mark it private (if the system is configured with that option).

- By default, Unity Connection relays private messages (as regular messages with the private flag) for users who have one or more message actions configured to relay messages to an SMTP relay address. To disable relaying of private messages, uncheck the Allow Relaying of Private Messages check box on the System Settings > Advanced > Messaging page in Cisco Unity Connection Administration.

Secure Messages

- Secure messages are stored only on the Unity Connection server, allowing you to control how long messages are retained before they are archived or permanently deleted. For secure messages, the Save Recording As option is automatically disabled on the Options menu on the Media Master in Cisco Unity Connection ViewMail for Microsoft Outlook (version 8.0), and Cisco Unity Connection ViewMail for IBM Lotus Notes.
- Secure messages can be useful for enforcing your message retention policy. You can configure Unity Connection to automatically delete secure messages that are older than a specified number of days, regardless of whether users have listened to or touched the messages in any way.
- Secure messages can be played by using the following interfaces:
  - Unity Connection phone interfaceCisco Unity Connection Web Inbox (Unity Connection 10.x) Cisco Unity Connection ViewMail for Microsoft Outlook (version 8.0)
  - Cisco ViewMail for Microsoft Outlook (version 8.5 and later)
  - Cisco Unity Connection ViewMail for IBM Lotus Notes
  - Cisco Unified Personal Communicator version 7.0 and later
  - Cisco Unified Mobile Communicator and Cisco Mobile
  - Cisco Unified Messaging with IBM Lotus Sametime version 7.1.1 and later. (For requirements for playing secure messages by using Cisco Unified Messaging with Lotus Sametime, see the applicable *Release Notes for Cisco Unified Messaging with IBM Lotus Sametime* at http://www.cisco.com/en/US/products/ps9830/prod_release_notes_list.html.)
- Secure messages can be forwarded by using the following interfaces:
  - Unity Connection phone interface
  - Cisco Unity Connection Unity Connection Web Inbox (in Unity Connection 10.x)
  - Cisco Unity Connection ViewMail for Microsoft Outlook 8.5
- Secure messages cannot be accessed by using the following interfaces:
  - IMAP clients (unless ViewMail for Outlook or ViewMail for Notes is installed)
  - RSS readers
- By default, only Unity Connection users who are homed on the local networking site can receive a secure message. VPIM contacts or users homed on a remote networking site may also be able to receive the message, but only when the VPIM location or intersite link is configured to allow secure message delivery. Message security cannot be guaranteed once a message leaves the Unity Connection site or is sent to a VPIM location.
- Replies to secure messages are also marked secure.
- A secure message can be forwarded to other Unity Connection users and to the Unity Connection users in a distribution list. The forwarded message is also marked secure. Users cannot change the sensitivity of forwarded messages and replies.
- When users sign in to Unity Connection and send a message, class of service settings determine whether the message is marked secure. By default, Unity Connection automatically marks a message secure when the user marks it private.

- *(Cisco Unity Connection 10.x)* If you want Unity Connection to announce to users that a message is marked secure, check the Announce Secure Status in Message Header check box on the System Settings > Advanced Settings > Conversation Configuration page. When the check box is checked, Unity Connection plays a prompt to the user before playing the secure message, announcing that it is a "...secure message...."
- When callers are routed to a user or call handler greeting and then leave a message, the Mark Secure check box on the Edit > Message Settings page for a user or call handler account determines whether Unity Connection marks the message secure.
- By default, Unity Connection does not relay secure messages for users who have one or more message actions configured to relay messages to an SMTP relay address. If a secure message is received for a user who is configured for relay, Unity Connection sends a non-delivery receipt to the sender. To have Unity Connection relay secure messages, check the Allow Relaying of Secure Messages check box on the System Settings > Advanced > Messaging page in Cisco Unity Connection Administration. Note that when the check box is checked, secure messages are relayed with a secure flag; however, most email clients will treat the messages as regular messages.
- Fax messages from the fax server are never marked secure.

ViewMail Limitations Regarding Secure Messages

- Secure messages cannot be forwarded by using Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 or ViewMail for IBM Lotus Notes.
- ViewMail for Outlook 8.0 and ViewMail for Notes support only playing secure messages.
- Messages that are composed or replied to by using ViewMail for Outlook 8.0 or ViewMail for Notes are not sent as secure, even when users are assigned to a class of service for which the Require Secure Messaging field is set to Always or to Ask.

Configuring Cisco Unity Connection to Mark All Messages Secure

Use the following Task List to configure Cisco Unity Connection to mark all messages secure:

1. Configure all classes of service to always mark messages secure. See the "To Enable Message Security for COS Members" procedure on page 11-3. (When users sign in to Unity Connection and send a message, class of service settings determine whether the message is marked secure.)
2. Configure user mailboxes to mark all outside caller messages secure. See the "To Configure Users and User Templates to Mark Messages Left By Outside Callers Secure" procedure on page 11-4.
3. Configure call handlers to mark all outside caller messages secure. See the "To Configure Call Handlers and Call Handler Templates to Mark Messages Left By Outside Callers Secure" procedure on page 11-4.
4. *(Cisco Unity Connection 10.x)* If you do not want Unity Connection to announce to users that a message is marked secure, uncheck the Announce Secure Status in Message Header check box on the System Settings > Advanced Settings > Conversation Configuration page.

To Enable Message Security for COS Members

Step 1 In Cisco Unity Connection Administration, find the COS that you want to change, or create a new one.

Step 2 On the Edit Class of Service page, under Message Options, in **Require Secure Messaging** list, select **Always.**

Step 3 Select **Save**.

Step 4 Repeat Step 1 to Step 3 for each class of service. Alternatively, you can edit multiple classes of services at once using the Bulk Edit option.

To Configure Users and User Templates to Mark Messages Left By Outside Callers Secure

Step 1 In Cisco Unity Connection Administration, find the user account or template that you want to edit.

If you want to edit multiple users at the same time, on the Search Users page, check the applicable user check boxes, and select **Bulk Edit**.

Step 2 On the Edit menu, select **Message Settings**.

Step 3 On the Edit Message Settings page, under Message Security, select the **Mark Secure** option.

If you are in Bulk Edit mode, you must first check the check box to the left of the **Mark Secure** field to indicate that you want to make a change to the field for the selected users or templates.

Step 4 Select **Save**.

To Configure Call Handlers and Call Handler Templates to Mark Messages Left By Outside Callers Secure

Step 1 In Cisco Unity Connection Administration, find the call handler or call handler template that you want to edit.

If you want to edit multiple call handlers at the same time, on the Search Call Handlers page, check the applicable call handler check boxes, and select **Bulk Edit**.

Step 2 On the Edit menu, select **Message Settings**.

Step 3 On the Edit Message Settings page, under Message Security check the **Mark Secure** check box.

If you are in Bulk Edit mode, you must first check the check box to the left of the **Mark Secure** field to indicate that you want to make a change to the field for the selected users.

Step 4 Select **Save**.

Shredding Message Files for Secure Delete

Some organizations require additional security in the deletion of messages, beyond having users simply delete them. The Message File Shredding Level setting on the Advanced Settings > Messaging Configuration page in Cisco Unity Connection Administration is a systemwide setting that ensures that the copy of the message being deleted by the user is securely deleted, by causing the message to be shredded the specified number of times when it is deleted. To enable the feature, you enter a setting other than 0 (zero). The setting that you enter in the field (a number from 1 through 10) indicates the number of times that the deleted message files are shredded. The shredding is done by way of a standard Linux shred tool: the actual bits that make up the message are overwritten with random bits of data the specified number of times.

By default, the shredding process occurs every 30 minutes when the Clean Deleted Messages sysagent task runs. Clean Deleted Messages is a read-only task; the configuration settings for the task cannot be changed. (Information about the task can be found in Cisco Unity Connection Administration under Tools > Task Management.)

There are some circumstances in which copies of messages or files that are associated with messages are not shredded:

- During the normal process of sending messages, temporary audio files are created. These temporary audio files are deleted when the message has been sent, but are not shredded. Any reference to the message is removed, but the actual data stays on the hard drive until the operating system has a reason to reuse the space and overwrites the data. In addition to these temporary audio files, there are other temporary files that are used during the delivery of a message that are deleted and shredded, if you have enabled shredding. Note that temporary files that are shredded are shredded immediately when the message they are associated with is deleted; unlike the message itself, the temporary files do not wait for the Clean Deleted Messages sysagent task to run.
- When a user attempts to play a message in the Web Inbox that is in a format that cannot be played, the message is transcoded into a temporary audio file. This temporary audio file is deleted when the user deletes the message, but it is not shredded.
- Shredding can occur only on messages that reside on the Unity Connection server. To ensure that messages are not recoverable from other servers, you should not use the following features: message relay, IMAP, ViewMail for Outlook, ViewMail for Notes, the Web Inbox, single inbox, the SameTime Lotus plug-in, Cisco Unified Personal Communicator, Cisco Mobile, or SMTP Smart hosts in between networked servers. If you want to use these features, you should also use the secure messaging feature. When you use secure messaging, there are no local copies of the secure messages, and users are not allowed to save local copies; therefore, all copies of messages remain on the Unity Connection server, and can thus be shredded when deleted.

  Note For additional information about secure messaging, see the "Secure Messages" section on page 11-2.

- Messages that are sent between locations in a Unity Connection network are written to a temporary location before they are sent. The temporary copies of the messages are deleted, but not shredded.

If you have enabled shredding in a Cisco Unity Connection cluster, messages are shredded on both the primary and secondary server when they are deleted.

We strongly recommend that you set the shredding level no higher than 3, due to performance issues.

Note that messages are shredded only when they have been hard deleted.

Message Security Options for IMAP Client Access in Cisco Unity Connection

When users access voice messages that are marked with normal or private sensitivity from an IMAP client, the IMAP client may allow users to save messages as WAV files to their hard disks, and may allow users to forward the messages. To prevent users from saving and/or forwarding voice messages from their IMAP client, consider specifying one of the following class of service options:

- Users can access only message headers in an IMAP client—regardless of message sensitivity.

- Users can access message bodies for all messages except those that are marked private. (Secure messages cannot be accessed in an IMAP client, unless the client is Microsoft Outlook and ViewMail for Outlook is installed or the client is Lotus Notes and ViewMail for Notes is installed.)