Messages

This chapter contains the following sections:

IMAP E-Mail Access to Cisco Unity Connection Voice Mail

See the following sections:

Changing Passwords

If users change a Cisco Unity Connection password from the Cisco Unity Assistant, they also must update this password from their IMAP e-mail client application so that the client can continue to access Connection and retrieve voice messages.

Troubleshooting Logon Problems with IMAP E-Mail Clients

If users have trouble receiving voice messages to their IMAP client, consider the following information:

- If the IMAP client application prompts a user for the Cisco PCA password, but does not accept it, the Cisco PCA password may have expired or changed, or is locked. Users can change their password from the Cisco Unity Assistant first and then update it from their IMAP client application.

- If Microsoft Outlook users are not prompted for their Cisco PCA password, verify that the Remember Password check box on the Internet E-mail Settings (IMAP) page is not checked. If this option is checked, and the password of the user has expired, changed, or is locked, Microsoft Outlook will not prompt the user to enter the Cisco PCA password. The result is that the user will not receive voice messages from Connection.

Message Quota Enforcement: Responding to Full Mailbox Warnings

When users hear a prompt about a full mailbox, it means that one or more of the three quotas that limit the size of voice mailboxes has been reached:

- If a mailbox has reached the size of the warning quota, the user will hear a warning that the mailbox is almost full.
- If a mailbox has reached the size of the send quota, the user will be unable to send messages and will hear that messages cannot be sent. If the user belongs to the correct class of service and has deleted messages in the mailbox, Cisco Unity Connection will offer the option to remove all deleted messages.
- If a mailbox has reached the size of the send and receive quotas, the user will experience the same conditions as the send quota and in addition will not be able to receive new messages. Unidentified caller messages will not be allowed, and messages from other users will generate nondelivery receipts to the senders. To decrease the size of the mailbox, the user can remove all deleted messages and/or remove saved or new messages individually until the mailbox size is below the quotas.

Undeliverable Messages

Occasionally, messages cannot be delivered to the recipient that the caller intended to reach. The system behavior in this case depends on the type of sender and the reason that the message could not be delivered.

In general, if Connection cannot deliver the message because of issues that are not likely to be resolved (for example, the caller was disconnected before addressing the message, or the recipient mailbox has been deleted), the message is sent to the Undeliverable Messages distribution list, and Connection sends a nondelivery receipt (NDR) to the sender.

Note that the sender will not receive a nondelivery receipt in the following cases:

- When the sender of the original message is an unidentified caller
- When the sender is a user, but the user is configured to not accept NDRs
- While the Microsoft SQL Server database is down (in this case, the NDR will be delivered when the database becomes available)

However, if the original message is malformed or contains non-voice messaging content, instead of sending the message to the Undeliverable Messages list, Connection will place the message in the MTA bad mail folder (UmssMtaBadMail). This folder is automatically checked nightly by the Monitor Bad Mail Folders task, and if messages are found, an error is written to the application event log indicating troubleshooting steps.

Caution Some tasks are critical to Connection functionality. Disabling or changing the frequency of critical tasks may adversely affect performance or cause Connection to stop functioning.

Messages Appear to Be Delayed

Use the "Task List for Troubleshooting Delay in Appearance of Messages" to troubleshoot the possible causes for the apparent delay of messages.

Task List for Troubleshooting Delay in Appearance of Messages

1. To confirm the arrival times of messages, generate a user message activity report for the user. For more information, see the "Generating System Configuration and Call Management Reports" chapter in the *Cisco Unity Connection System Administration Guide*, *Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
2. See the applicable information in the "Orientation Task List" section of the "User Orientation" chapter of the *Cisco Unity Connection User Setup Guide, Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Some Messages Seem to Disappear

Use the "Task List for Troubleshooting the Disappearance of Some Messages" to troubleshoot the possible causes for messages not being delivered to the intended recipients.

Task List for Troubleshooting the Disappearance of Some Messages

1. Verify that users who are assigned to the Undeliverable Messages distribution list have been forwarding messages to the intended recipients. See the "Undeliverable Messages Have Not Been Forwarded to Recipients" section on page 9-4.
2. Verify that the user mailbox is not full. See the "A User Has a Full Mailbox" section on page 9-3.
3. Confirm that you or another administrator did not inadvertently delete a user who was assigned to review the messages for Connection entities. See the "Users Assigned to Cisco Unity Connection Entities Were Deleted and No Replacements Were Assigned" section on page 9-4.
4. *If McAfee VirusScan is installed on the Connection server:* Confirm that the default setting to block traffic on SMTP port 25 has been changed. Blocking traffic on SMTP port 25 prevents Connection from delivering voice messages to user inboxes. See the "McAfee VirusScan Is Blocking Traffic on SMTP Port 25" section on page 9-5.
5. Review message aging settings. See the "Message Aging Policy" chapter in the *Cisco Unity Connection System Administration Guide*, at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

A User Has a Full Mailbox

If a user mailbox is no longer allowed to receive messages, Cisco Unity Connection handles the message in one of the two following ways:

- By default, if an outside caller attempts to send a message to a user whose send/receive quota has been exceeded, Connection will indicate to the caller that the recipient mailbox is full, and will not allow the caller to record a message for the recipient.

  If the recipient mailbox has not yet exceeded the send/receive quota at the time an unidentified caller records a message, but the quota is exceeded in the act of delivering the message, Connection will deliver the message regardless of the quota.

- If a user whose voice mailbox has exceeded the send quota logs in to Connection and attempts to send a message to another user, Connection will indicate that the send quota has been exceeded, and will not allow the sender to record the message. If the user calls another user and is forwarded to a voice mailbox, the user will be able to leave a message, but the message will be sent as an outside caller message.

  If a user attempts to send a message to another user whose mailbox has exceeded the send/receive quota, or if the quota is exceeded in the act of delivering the message, Connection will send a nondelivery receipt to the message sender.

  Connection delivers read receipts and nondelivery receipts to users regardless of whether their quotas have been exceeded.

Encourage the user to dispose of messages promptly so that the Connection mailbox does not fill up, and explain to users on the Undeliverable Messages distribution list the importance of regularly checking for and forwarding undeliverable messages.

Caution If the mailbox(es) of the user(s) who are assigned to check the Undeliverable Messages list exceed the send/receive quota, the messages sent to the Undeliverable Messages distribution list are lost. To avoid this problem, specify a generous value for the send/receive quota for at least one user who is a member of the Undeliverable Messages list, and encourage the user to dispose of messages promptly.

Undeliverable Messages Have Not Been Forwarded to Recipients

Messages returned to the Unity Messaging System mailbox are forwarded automatically to users whose names appear on the Undeliverable Messages system distribution list. The messages then must be forwarded to the intended recipients. Explain to users on the Undeliverable Messages distribution list the importance of regularly checking for and forwarding undeliverable messages.

Caution If the mailbox(es) of the user(s) who are assigned to check the Undeliverable Messages list exceed the send/receive quota, the messages sent to the Undeliverable Messages distribution list are lost. To avoid this problem, specify a generous value for the send/receive quota for at least one user who is a member of the Undeliverable Messages list, and encourage the user to dispose of messages promptly.

Users Assigned to Cisco Unity Connection Entities Were Deleted and No Replacements Were Assigned

When you delete a user who was assigned to review the messages sent to any of the following Cisco Unity Connection entities, make sure that you assign another user or a distribution list to replace the deleted user; otherwise, messages may be lost.

- Undeliverable Messages distribution list (by default, the UndeliverableMessagesMailbox user account is the only member of this distribution list)

- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

McAfee VirusScan Is Blocking Traffic on SMTP Port 25

By default, McAfee VirusScan Enterprise blocks traffic on SMTP port 25, which prevents Cisco Unity Connection from delivering voice messages to user inboxes. When this occurs, you may see the following error in the Windows application event log:

Event Type: Error
Event Source: CiscoUnity_CsMalUmss
Event Category: Error
Event ID: 1004
Date: <date>
Time: <time>
User: N/A
Computer: <server name>
Description: The SMTP service on localhost:25 is not responding and is unable to deliver messages. The SMTP service may be down. Messages will accumulate in [drive letter]:\UC_Mailroot\UmssCsMalQueue until this is resolved. Verify that the SMTP service is running.

To change the setting in VirusScan, do the following procedure. Note that the procedure is current as of the time this document was written. The VirusScan user interface may change.

To Stop McAfee VirusScan from Blocking Traffic on SMTP Port 25

Step 1 Start McAfee VirusScan Console.

Step 2 Right-click **Access Protection**, and click **Properties**.

Step 3 In the Access Protection Properties dialog box, on the Port Blocking tab, in the Ports to Block list, confirm that the **Prevent Mass Mailing Worms From Sending Mail** check box is unchecked.

Step 4 Click **OK** to close the Properties dialog box.

Step 5 Close the VirusScan Console.

Cisco Unity Connection Stops Recording Before a Caller Has Finished Leaving a Message

If a caller reports being cut off while leaving a message and if the caller did not hear a prompt prior to the disconnect, Cisco Unity Connection, the phone system, or the central office may have disconnected the call.

To Determine Why the Call Was Disconnected

Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.

Step 2 In the left pane of Event Viewer, click **System Log**.

Step 3 In the system event log, look for an error that occurred at the time of the reported disconnected call.

If an error appears, double-click the error and skip to Step 6.

If no error appears for the date and time of the disconnected call, continue with Step 4.

Step 4 In the left pane, click **Application Log**.

Step 5 In the application event log, look for an error that occurred at the time of the reported disconnected call. Double-click the error.

Step 6 In the Event Detail dialog box, review the contents of the Description box.

If you need assistance interpreting or resolving the error, or if no error appears in the application event log that matches the date and time of the reported disconnected call, contact Cisco TAC.

Secure Messages

A user who is enabled to send encrypted secure messages will hear "To mark this private and secure, press 3" in the Cisco Unity Connection conversation while sending a message. The message will be encrypted, and marked private to prevent it from being forwarded. A user who is not enabled to send encrypted secure messages will instead hear "To mark this private, press 3," which will prevent the message from being forwarded. A user also can mark a message both private and secure in the Cisco Personal Communications Assistant.

A user may not need to explicitly mark a message for encryption. There are several system-level settings that control whether a message is encrypted. A system-level setting can be enabled so that all user-to-user messages are encrypted or that all outside-caller messages are encrypted.

See the following troubleshooting sections for more information on these issues:

- An encryption or decryption error results in the generation of an Event log error message. See the "Decryption Event Log Error Messages" section on page 9-6 or the "Encryption Event Log Error Messages" section on page 9-7, as applicable.
- A user hears the failsafe conversation or the decoy WAV file. See the "Users Hear the Failsafe Conversation or the Decoy WAV File" section on page 9-7.

Note For more information on private and secure messaging, see the "Setting Up Private and Secure Messaging" chapter of the *Cisco Unity Connection System Administration Guide*, *Release 1.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Decryption Event Log Error Messages

Decryption errors can be caused by the following:

- The voice message was not encrypted with the public key.
- The private key is missing, invalid, or unable to be used.
- There is another problem with the key.

In all of these cases, start by creating a new certificate. Then ask the sending user to re-record the voice message, if applicable.

Error Message `A private secure message from %ss to %sr could not be decrypted, possibly because the message was not encrypted with the public key for this server or there is a problem with the private key on this server.`

Recommended Action Install a new certificate on the Connection server, and restart Connection services. If this does not resolve the problem, contact Cisco TAC.

Encryption Event Log Error Messages

Encryption errors are caused by a problem with the public key. For example, the public key may be missing, invalid, or unusable. Start by creating a new certificate. Then ask the sending user to re-record the voice message, if applicable.

Error Message `A private secure message from %ss could not be encrypted because a valid public key could not be found on this server.`

Recommended Action Create a new certificate on this server, then ask the sending user to re-record the voice message. If creating a new certificate on this server does not resolve the problem, contact Cisco TAC.

Error Message `A private secure message from %ss could not be encrypted, possibly because there is a problem with the public key on this server.`

Recommended Action Create a new certificate on this server, then ask the sending user to re-record the voice message. If creating a new certificate on the sending server does not resolve the problem, contact Cisco TAC.

Users Hear the Failsafe Conversation or the Decoy WAV File

If a user hears the failsafe conversation (“Sorry, this system is temporarily unable to take your call”) when attempting to send a secure voice message, encryption of the message may have failed. Review the Windows application event log to determine the cause. When an encryption attempt fails, the voice message is deleted and cannot be recovered. The user must re-record the message.

If a user hears the following decoy WAV file when attempting to listen to a secure voice message by phone, decryption of the message may have failed:

> “This voice message is private and secure and can only be played if you log on to the voice mail system and check your messages by phone. If you received this message in error, notify the sender and delete it immediately.”

Review the application event log to determine the cause. When a decryption attempt fails, in most cases the voice message will not be playable, even after the problem has been resolved. For example, when problem resolution requires creation of a new certificate on the Connection server, then the sending user must re-record the message.