CHAPTER 21

Configuring IMAP Settings in Cisco Unity Connection 9.x

This chapter contains information on setting up Cisco Unity Connection so that users can use IMAP clients to send, forward, or reply to messages through the Connection server.

See the following sections:

- Overview of SMTP Message Handling in Cisco Unity Connection 9.x, page 21-1
- Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook 9.x, page 21-2
- Recommendations for Deploying IMAP Access in Cisco Unity Connection 9.x, page 21-3
- Task List for Configuring IMAP Access in Cisco Unity Connection 9.x, page 21-3
- Procedures for Configuring IMAP Access in Cisco Unity Connection 9.x, page 21-5

Overview of SMTP Message Handling in Cisco Unity Connection 9.x

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

When an authorized IMAP client tries to send a message to Connection through SMTP, Connection attempts to categorize the message as a voicemail, email, fax, or delivery receipt. Connection also attempts to map the sender to a user and the message recipients to users or contacts by comparing the SMTP addresses in the message header to its list of SMTP proxy addresses.

If SMTP authentication is configured for the IMAP client and the SMTP address of the sender matches a proxy address or the primary SMTP address for the authenticated user, or 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 Connection user, Connection processes the message for each individual recipient based on the type of recipient:

- If the recipient maps to a VPIM contact, Connection converts the message into a VPIM message, removing any attachment that is not allowed by the VPIM standard. Then, 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 Connection server for delivery if the VPIM location is homed on that server.

- If the recipient maps to a user homed on the local server, 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 Connection accepts the message and places it in the user mailbox on the 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 Connection server, Connection relays the message to the home server of the user, which then performs the action specified on the Message Actions page of the user profile.
- If the recipient does not map to any of the above, 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 Connection Administration. By default, 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 Connection server returns an SMTP error, which in most cases 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, Connection puts the message into the MTA bad mail folder (UmssMtaBadMail).

Note that Connection marks an incoming SMTP message as secure if the message includes the secure header, or if the message sender is a user who is in a class of service that is configured to always send secure messages. See the "How Cisco Unity Connection 9.x Handles Messages That Are Marked Private or Secure" section in the "Securing User Messages in Cisco Unity Connection 9.x" chapter of the *Security Guide for Cisco Unity Connection Release 9.x at* http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.)

Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook 9.x

The employees at ExampleCo use 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 Cisco 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 plug-in. The Outlook client for each employee is configured to access the Connection user account via 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. 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, which 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. In this case, because ViewMail is configured to use the Connection IMAP account to send messages, the voice message is routed to the Connection server for delivery.

When 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). Because these addresses are defined as SMTP proxy addresses for the user profiles of Robin Smith and Chris Jones respectively, Connection delivers the message as a voice message from Robin Smith to Chris Jones.

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 Connection account that Chris accesses via IMAP. If Chris replies to either message, the Outlook client will automatically route the reply by using the account in which Chris received the original message.

Note that because Connection is configured to be able to match the corporate email addresses in use at ExampleCo to Connection user accounts (via the SMTP proxy address that is defined for each user), users can use the existing Outlook address book to address both email and voice messages. In addition, users do not need to think about which account to use to compose, reply to, or forward messages—this is all handled automatically by the Outlook and ViewMail configuration.

Recommendations for Deploying IMAP Access in Cisco Unity Connection 9.x

When deploying IMAP clients to access and send Cisco Unity Connection messages, we recommend the following:

- Use a firewall to protect the Connection 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 Connection IMAP account on user workstations, use the corporate email address of the user, rather than the Connection-specific email address, in the IMAP settings. In this way, users do not need to know an extra set of email addresses for addressing voice messages in the email client, and are insulated from changes to the Connection-specific addresses if the Connection SMTP domain is changed.

Note The corporate email address mentioned in the SMTP Proxy Address should not be the same with the email address mentioned in the Accept and Relay option of any other user.

- ViewMail for Outlook limits the message recipients that a user can reach to objects that are in the search space of the user, and sends a non-delivery receipt (NDR) for messages that are sent to recipients that do not appear in the 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, consider creating a separate Outlook address book for ViewMail users that is limited to the objects in the user search space.

Task List for Configuring IMAP Access in Cisco Unity Connection 9.x

1. *If you plan to configure Cisco Unity Connection to relay messages for users to another SMTP server,* do the following subtasks:
   a. Configure the SMTP smart host to accept messages from the Connection server. See the documentation for the SMTP server application that you are using.

   b. Configure the Connection server to relay messages to the smart host. See the "Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host" section on page 21-5.

   c. Review the settings that control whether private or secure messages can be relayed. See the "Configuring Message Relay Settings" section on page 21-5.

2. Configure message actions for Connection users or user templates. See the "Message Actions in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

3. Configure SMTP proxy addresses for users who will send or receive messages from IMAP clients.See the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Note At a minimum, we recommend that you configure the corporate email address of each user as an SMTP proxy address for the user.

4. Associate users with a class of service that offers a license to use an IMAP client to access voice messages. See the "IMAP Client Access to Voice Messages in Cisco Unity Connection 9.x" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service Settings in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

5. Configure SMTP proxy addresses for VPIM contacts who may receive messages from IMAP clients. See the "SMTP Proxy Addresses in Cisco Unity Connection 9.x" section in the "Managing Contacts in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

6. Configure the Connection server to allow SMTP connections from IMAP clients. See the "Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication" section on page 21-6.

7. *If you configured Transport Layer Security to be required or optional in the procedure in Task* 6.: Configure the Connection server to provide a secure IMAP connection, as described in the "Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 9.x" section on page 26-2.

8. Optionally, modify the settings that determine the characteristics of SMTP messages that Connection accepts. See the "Configuring SMTP Message Parameters" section on page 21-7.

9. For each user workstation, configure a supported IMAP client to access a Connection mailbox.See the "Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Procedures for Configuring IMAP Access in Cisco Unity Connection 9.x

See the following sections:

- Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication, page 21-6
- Configuring Message Relay Settings, page 21-5
- Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication, page 21-6
- Configuring SMTP Message Parameters, page 21-7

Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host

To enable Cisco Unity Connection to relay any type of message to the SMTP address for a user, your Connection server must be configured to relay messages through a smart host.

To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

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

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

Step 3 Select **Save**.

Configuring Message Relay Settings

You can choose whether Cisco Unity Connection relays messages that are marked private or secure.

To Configure Message Relay Settings

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

Step 2 To have Cisco Unity Connection relay messages that are marked private, check the **Allow Relaying of Private Messages** check box. (This check box is checked by default.) Connection sets the private flag on the message when relaying a private message.

To prevent Connection from relaying private messages, uncheck the check box. Connection sends an NDR to the message sender when it receives a message that it cannot relay because the message is marked private.

Step 3 To have Connection relay secure messages, check the **Allow Relaying of Secure Messages** check box. (This check box is unchecked by default.) Connection relays secure messages as regular messages.

To prevent Connection from relaying secure messages, uncheck the check box. Connection sends an NDR to the message sender when it receives a message that it cannot relay because the message is marked secure.

Step 4 Select **Save**.

Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication

You have a number of options for controlling which clients can initiate SMTP connections with Cisco Unity Connection. You can create an access list, which allows you to configure specific IP addresses or IP address patterns that correspond with clients that you wish to allow or deny access. You can also choose to allow all clients to connect, regardless of IP address; if you do so, you can specify whether those clients (known as untrusted IP addresses) must authenticate, and whether Transport Layer Security is required or allowed for clients with untrusted IP addresses.

If you choose to require clients with untrusted IP addresses to authenticate with Connection, users enter their Connection alias and Cisco PCApassword (also known as the web-application password) in the IMAP client to authenticate. Make sure that users understand that whenever they change their Cisco PCA password in the Connection Messaging Assistant, they also must update the password in their IMAP client. If users have trouble receiving voice messages in an IMAP client after having updated their Cisco PCA password in both applications, see the “Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection 9.x” section in the “Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages” chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 9.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Do one or both of the following procedures, as applicable.

- To Configure the Cisco Unity Connection IP Address Access List, page 21-6
- To Configure Access and Authentication for Untrusted IP Addresses, page 21-7

To Configure the Cisco Unity Connection IP Address Access List

---

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

Step 2 On the SMTP Server Configuration page, on the Edit menu, select **Search IP Address Access List**.

Step 3 On the Search IP Address Access List page, select **Add New** to add a new IP address to the list.

Step 4 On the New Access IP Address page, enter an IP address; or, you can enter a single * (asterisk) to match all possible IP addresses.

Step 5 Select **Save**.

Step 6 On the Access IP Address page, to allow connections from the IP address that you entered in Step 4, check the **Allow Connection** check box. To reject connections from this IP address, uncheck the check box.

Step 7 If you have made any changes on the Access IP Address page, select **Save**.

Step 8 Repeat Step 2 through Step 7 for each additional IP address that you want to add to the access list.

To Configure Access and Authentication for Untrusted IP Addresses

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

Step 2 On the SMTP Server Configuration page, check the **Allow Connections From Untrusted IP Addresses** check box to allow all clients to connect by using SMTP, regardless of whether Connection is configured to specifically allow connections from their IP addresses.

Step 3 If you checked the check box in Step 2, check the **Require Authentication From Untrusted IP Addresses** check box to configure authentication for these types of clients. Then, select how Connection handles Transport Layer Security for untrusted IP addresses:

- Disabled—Connection does not offer TLS as an option for SMTP sessions that are initiated by clients or servers with untrusted IP addresses. In most cases, if the client is configured to use TLS, but Connection does not offer it, the connection fails and the client notifies the user.
- Required—Clients or servers connecting from untrusted IP addresses must use TLS to initiate SMTP sessions with the Connection server.
- Optional—Clients or servers connecting from untrusted IP addresses can use TLS to initiate SMTP sessions with the Connection server, but are not required to do so.

Note To protect user passwords, we recommend that you require authentication from untrusted IP addresses and configure Transport Layer Security as either Required or Optional.

Step 4 If you chose Required or Optional for the Transport Layer Security setting in Step 3, to configure TLS on the Connection server, see the "Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 9.x" section on page 26-2.

Configuring SMTP Message Parameters

You can configure Connection to reject any incoming SMTP messages that are larger than a configurable total size or have more than a configurable number of recipients. By default, Connection accepts messages that are larger than 10 MB or have more than 15,000 recipients.

To Configure SMTP Message Parameters

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

Step 2 On 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.

Step 4 Select **Save**.