Configuring Cisco Unity Connection and Microsoft Office 365 for Unified Messaging

See the following sections:

About Unified Messaging with Office 365 in Cisco Unity Connection

See the following sections:

Accessing Office 365 Email by Using Text to Speech in Cisco Unity Connection

When Cisco Unity Connection is configured to allow access to Office 365 email by using text to speech, users have the option to hear their emails read to them when they sign in to Cisco Unity Connection by phone.

Accessing Office 365 Calendars and Contacts in Cisco Unity Connection

When Cisco Unity Connection is configured to access Office 365 calendars and contacts, Connection users can do the following by phone:

- Hear a list of upcoming meetings (Outlook meetings only).
- Hear a list of the participants for a meeting.
- Send a message to the meeting organizer.
- Send a message to the meeting participants.
- Accept or decline meeting invitations (Outlook meetings only).
- Cancel a meeting (meeting organizers only).

In addition, Connection enables users to import Office 365 contacts by using the Connection Messaging Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Connection Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

Synchronizing Voice Messages in Connection and Office 365 Mailboxes in Cisco Unity Connection (Single Inbox)

Revised September 13, 2013

If any unified users' Exchange mailboxes have more than 1000 messages, which includes voice messages and receipts, then enable the EWS paged view search functionality at Cisco Unity Connection. For more information on the paged view search functionality, see the "Configuring EWS Limits for the Unified Messaging Users for Cisco Unity Connection (Exchange 2013 and Later)" section of the "Configuring Cisco Unity Connection and Microsoft Exchange for Unified Messaging" chapter of this guide.

This section describes how synchronizing voice messages in Connection and Office 365 mailboxes works. See the following sections:

Where Voice Messages Are Stored When Single Inbox Is Configured

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

How Single Inbox Works With ViewMail for Outlook

If you want users to use Outlook to send new Connection voice messages, or to reply to or forward voice messages, and if you want the messages to be synchronized with Connection:

- If you have not already done so, in Connection Administration, add SMTP proxy addresses for the Connection users that are configured for single inbox. The SMTP proxy address for a user must match the Office 365 email address that is specified in the unified messaging account in which single inbox is enabled.
- Install ViewMail for Outlook on user workstations. Without ViewMail for Outlook installed, voice messages are sent by Outlook as emails with .wav file attachments, and are treated as emails by Connection.
- On each user workstation, associate an email account with a Connection server.

Voice messages appear in the Outlook Inbox folder of the user, alongside other messages that are stored in Office 365; the voice messages also appear in the Connection mailbox of the user.

When single inbox is configured, Connection adds a Voice Outbox folder to the Outlook mailbox. Connection voice messages sent from Outlook do not appear in the Sent Items folder.

Private messages cannot be forwarded.

How Single Inbox Works without ViewMail for Outlook or with Other Email Clients

If you use another email client to access Connection voice messages in Office 365, or if you do not install ViewMail for Outlook:

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

Accessing Secure Voice Messages in the Exchange Mailbox

To play secure Connection voice messages in the Exchange mailbox, users must use Microsoft Outlook and Cisco Unity Connection ViewMail for Microsoft Outlook. Without ViewMail for Outlook installed, users accessing secure voice messages see only text in the body of a decoy message; the text briefly explains secure messages.

How Synchronization Works With Outlook Folders

Connection synchronizes voice messages in the following Outlook folders with the Connection Inbox folder for the user, so the messages are still visible in the Connection Inbox folder:

- Subfolders under the Outlook Inbox folder
- Subfolders under the Outlook Deleted Items folder
- The Outlook Junk Email folder

Messages in the Outlook Deleted Items folder appear in the Connection deleted items folder.

If the user moves voice messages (except secure voice messages) into Outlook folders that are not under the Inbox folder, the messages are moved to the deleted items folder in Connection. The messages can still be played by using ViewMail for Outlook because a copy still exists in the Outlook folder. If the user moves the messages back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Connection Inbox folder, and:

- If the message is still in the deleted items folder in Connection, the message is synchronized back into the Connection Inbox for that user.
- If the message is not still in the deleted items folder in Connection, the message is still playable in Outlook, but it is not resynchronized into Connection.

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

If the user moves a secure message to an Outlook folder that is not synchronized with the Connection Inbox folder, the only copy of the voice message is moved to the deleted items folder in Connection, and the message can no longer be played in Outlook. If the user moves the message back into the Outlook Inbox folder or into an Outlook folder that is synchronized with the Connection Inbox folder, and:

- If the message is still in the deleted items folder in Connection, the message is synchronized back into the Connection Inbox for that user, and the message becomes playable again in Outlook.
- If the message is not still in the deleted items folder in Connection, the message is not resynchronized into Connection and can no longer be played in Outlook.

Where Deleted Messages Go

By default, when a user deletes a voice message in Connection, the message is sent to the Connection deleted items folder and synchronized with the Outlook Deleted Items folder. When the message is deleted from the Connection deleted items folder (the user can do this manually, or you can configure message aging to do it automatically), it is also deleted from the Outlook Deleted Items folder.

If you are adding the single-inbox feature to an existing system, and if you have configured Connection to permanently delete messages without saving them in the deleted items folder, messages that users delete by using the Web Inbox or by using the Connection phone interface are still permanently deleted.

However, messages that users delete by using Outlook are only moved to the Deleted Items folder in Outlook, not permanently deleted. When Connection synchronizes with Office 365, the message is moved to the Connection deleted items folder; it is not permanently deleted. We recommend that you do one or both of the following:

- Configure message aging to permanently delete messages in the Connection deleted items folder.

- Configure message quotas, so that Connection prompts users to delete messages when their mailboxes approach a specified size.

When a user deletes a voice message from any Outlook folder, including the Outlook Inbox folder, the Deleted Items folder, or any subfolder, the message is moved to the deleted items folder in Connection. No operation in Outlook will cause a message to be permanently deleted in Connection.

Types of Connection Messages That Are Not Synchronized with Office 365

The following types of messages are not synchronized:

- Sent messages

- Draft messages

- Messages configured for future delivery but not yet delivered

- Broadcast messages

- Unaccepted dispatch messages. When a dispatch message has been accepted by a recipient, it becomes a normal message and is synchronized with Office 365 for the user who accepted it and deleted for all other recipients. Until someone on the distribution list accepts a dispatch message, the message waiting indicator for everyone on the distribution list will remain on, even when users have no other unread messages.

Replication of Status Changes

Status changes (for example, from unread to read), changes to the subject line, and changes to the priority are replicated from Connection to Exchange and vice versa, as applicable.

How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes

When you configure unified messaging, you create one or more unified messaging services that define, among other things, which unified messaging features are enabled. You also create one or more unified messaging accounts for each user to associate the user with unified messaging services. You can disable single inbox in three ways:

- Entirely disable a unified messaging service in which single inbox is enabled. This disables all enabled unified messaging features (including single inbox) for all users that are associated with the service.

- Disable only the single inbox feature for a unified messaging service, which disables only the single inbox feature for all users that are associated with that service.

- Disable single inbox for a unified messaging account, which disables single inbox only for the associated user.

If you disable and later re-enable single inbox by using any of these methods, Connection resynchronizes the Connection and Office 365 mailboxes for the affected users. Note the following:

- If users delete messages in Office 365 but do not delete the corresponding messages in Connection while single inbox is disabled, the messages will be resynchronized into the Office 365 mailbox when single inbox is re-enabled.

- If messages are hard deleted from Office 365 (deleted from the Deleted Items folder) before single inbox is disabled, the corresponding messages that are still in the deleted items folder in Connection when single inbox is re-enabled will be resynchronized into the Office 365 Deleted Items folder.

- If users delete messages in Connection but do not delete the corresponding messages in Office 365 while single inbox is disabled, the messages remain in Office 365 when single inbox is re-enabled. Users must delete the messages from Office 365 manually.

- If users change the status of messages in Office 365 (for example, from unread to read) while single inbox is disabled, the status of Office 365 messages will be changed to the current status of the corresponding Connection messages when single inbox is re-enabled.

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

How Read/Heard Receipts, Delivery Receipts, and Non-delivery Receipts Are Synchronized

Connection can send heard/read receipts, delivery receipts, and non-delivery receipts to Connection users who send voice messages. If the sender of a voice message is configured for single inbox, the applicable receipt is sent to the Connection mailbox for the sender. The receipt is then synchronized into the Office 365 mailbox for the sender.

Note the following.

- *Read/heard receipts:* When sending a voice message, a sender can request a read/heard receipt. If you do not want Connection to respond to requests for read receipts, in Connection Administration, uncheck the Respond to Requests for Read Receipts check box, which appears on the Users > Users > Edit > Mailbox page and on the Templates > User Templates > Edit > Mailbox page.

- *Delivery receipts:* A sender can request a delivery receipt only when sending a voice message from ViewMail for Outlook. You cannot prevent Connection from responding to a request for a delivery receipt.

- *Non-delivery receipts (NDR):* A sender receives an NDR when a voice message cannot be delivered. If you do not want Connection to send an NDR when a message cannot be delivered, in Connection Administration, uncheck the Send Non-Delivery Receipts for Message Failed Delivery check box, which appears on the Users > Users > Edit User Basics page and on the Templates > User Templates > Edit User Template Basics page.

    Note the following about NDRs:

    – When the sender accesses Connection by using the TUI, the NDR includes the original voice message, which allows the sender to resend the message at a later time or to a different recipient.

    – When the sender accesses Connection by using Web Inbox, the NDR includes the original voice message, but the sender cannot resend it.

    – When the sender uses ViewMail for Outlook to access Connection voice messages that have been synchronized into Office 365, the NDR is a receipt that contains only an error code, not the original voice message, so the sender cannot resend the voice message.

    – When the sender is an outside caller, NDRs are sent to Connection users on the Undeliverable Messages distribution list. Verify that the Undeliverable Messages distribution list includes one or more users who regularly monitors and reroutes undelivered messages.

Task List for Configuring Cisco Unity Connection and Office 365 for Unified Messaging

To configure one or more unified messaging features, complete the following tasks in the order presented.

1. Review the "Requirements for Using Unified Messaging Features" section in the *System Requirements for Cisco Unity Connection Release 9.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/requirements/9xcucsysreqs.html .

2. *Cisco Unified Communications Manager Business Edition only:* Confirm that Connection is licensed for single inbox. See the "Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only)" section on page 3-10

3. *If Connection is integrated with an LDAP directory:* Review the current LDAP directory configurations to confirm that the Cisco Unified Communications Manager Mail ID field is synchronized with the LDAP mail field. During the integration process, this causes values in the LDAP mail field to appear in the Corporate Email Address field in Connection.

    Unified messaging requires that you enter the Office 365 email address for each Connection user. On the Unified Messaging Account page, each user can be configured to use either of the following values:

    –   The Corporate Email Address specified on the User Basics page

    –   The email address specified on the Unified Messaging Account page

    Email address field on the Unified Messaging Account page can be populated by using Connection Administration or the Bulk Administration Tool.

> **Note**   Connection supports on-premise LDAP directory integration only.

4. *If you are using single inbox and you want users to be able to use ViewMail for Outlook to send new voice messages, or to forward or reply to voice messages:* Install Cisco Unity Connection ViewMail for Microsoft Outlook on user workstations. For more information on installing ViewMail for Outlook, see the *Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook Release 8.5(x)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

5. Synchronization threads configuration should be done based on latency between Connection and Office 365 server. For more information, refer to "Latency" section of the design guide at

    http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/design/guide/8xcucdg032.html.

6. Decide whether you want Connection to be able to search for and communicate with different Office 365 server, or you want Connection to communicate with a specific Office 365 server in case the hostname or the IP Address of the specific Office 365 server is known**. Auto Discovery is the recommended option**.

    If Connection is not already configured to use DNS, use the following CLI commands to configure DNS:

    –   set network dns

    –   set network dns options

    We recommend that you configure Connection to use the same DNS environment in which the Active Directory environment is publishing its records.

For more information on the CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at
http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

7. Create an Active Directory account to be used for Connection unified messaging services, and grant the account the applicable permissions. See the "Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection" section on page 3-10.

8. If you are using single inbox and users do not already have added SMTP proxy addresses: Add proxy addresses to Connection user accounts. For more information, 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*, available at
http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

9. Update class of service settings as required:

   – Enable single inbox in one or more classes of service. For more information, see the "Single Inbox in Cisco Unity Connection" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at
   http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

   Note that all users who are configured to use single inbox must be in a class of service in which single inbox is enabled.

   Cisco Unified Communications Manager Business Edition only: Connection counts all users in a class of service in which single inbox is enabled as single inbox users even if they are not configured to use single inbox. For example, if a Connection server is licensed for 200 single-inbox users, and if you have three classes of service in which single inbox is enabled, the total number of users assigned to those three classes of service cannot exceed 200 users. This is true even if you only configure 50 users to use single inbox.

   – Enable text-to-speech access to Exchange voice messages on one or more classes of service: check the Allow Access to Advanced Features check box on the applicable class of service page, and then check the Allow Access to Exchange Email by Using Text to Speech (TTS) check box.

10. *If classes of service for single-inbox users have Delete Messages Without Saving to Deleted Items Folder enabled:* We recommend that you configure message aging and/or message quotas. Otherwise, messages deleted from Outlook may never be permanently deleted from Connection. For more information, see the "Synchronizing Voice Messages in Connection and Office 365 Mailboxes in Cisco Unity Connection (Single Inbox)" section on page 3-2.

   For more information on configuring message aging and message quotas for Connection, see the "Controlling the Size of Mailboxes in Cisco Unity Connection 9.x" chapter in the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at
   http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

11. Configure one or more Connection unified messaging services. See the "Creating a Unified Messaging Service to Access Office 365 from Cisco Unity Connection" section on page 3-12.

12. *Selected configurations:* For the following configuration, upload SSL certificates on the Connection server to encrypt communication between Connection and Office 365 and between Connection and Active Directory:

- If you configured Connection to search for and communicate with different Exchange servers, to use LDAPS to communicate with domain controllers, and to validate certificates for domain controllers in Task 10.

⚠️

Caution   When you allow Connection to search for and communicate with Office 365 servers, Connection communicates with Active Directory servers using Basic authentication. By default, the user name and password of the unified messaging services account and all other communication between the Connection and Active Directory servers is sent in clear text. If you want this data to be encrypted, in Task 11. you must configure unified messaging services to communicate with Active Directory domain controllers by using the secure LDAP (LDAPS) protocol.

For more information, see the Uploading CA Public Certificates for Exchange and Active Directory Servers to the Cisco Unity Connection Server, page 2-40.

13. Test the unified messaging configuration. See the following sections:

    - Testing Unified Messaging Services for Cisco Unity Connection, page 3-14
    - Testing Unified Messaging Accounts for Cisco Unity Connection, page 3-15
    - Testing System Configuration, Including Unified Messaging, with Office 365 and Cisco Unity Connection, page 3-15
    - Testing Access to Office 365 Calendars for Cisco Unity Connection, page 3-16

14. *If Connection voice messages are automatically being moved to the Outlook Junk Items folder:* Change the Outlook configuration to add the sender of the voice message or the sender's domain to the safe sender's list. For more information, see Outlook Help.

15. To teach users how to use the Connection calendar, refer them to the following:

    - For listing, joining, and scheduling meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/phone/b_9xcucu gphone.html.
    - For importing Exchange contacts, see the "Managing Your Personal Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/assistant/b_9xcu cugasst.html.
    - For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user/guide/pctr/b_9xcucugp ctr.html.

✎

Note   Office 365 servers, which Connection accesses have authentication mode set to Basic and web-based protocol set to HTTPS.

Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection

Cisco Unity Connection accesses Office 365 mailboxes by using a domain service account called the unified messaging services account. After you create the account, you grant it the rights necessary for Connection to perform operations on behalf of the user.

See the following section:

Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection, page 3-10

Task list for Creating the Unified Messaging Services Account and Granting Permissions for Cisco Unity Connection

1. Create one or more service accounts on the Office 365 servers with which you want Connection to communicate. Note the following:

   – Give the account a name that identifies it as the unified messaging services account for Connection.

   – Do not add the account to any administrator group.

   – Do not disable the account, or Connection cannot use it to access Office 365 mailboxes.

   – Specify a password that satisfies the password-security requirements of your company. The password is encrypted with AES 128-bit encryption and stored in the Connection database. The key that is used to encrypt the password is accessible only with root access, and root access is available only with assistance from Cisco TAC.

   – When you are configuring unified messaging for a Connection cluster, Connection automatically uses the same unified messaging services account for both Connection servers.

   – When you are configuring unified messaging for intersite networking or for intrasite networking, you can use the same unified messaging services account for more than one Connection server. However, this is not a requirement and does not affect functionality or performance.

2. For Assigning the Impersonation Rights to Service Accounts see the following Section,*Release 9.x* at Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only), page 3-10

Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 only)

Revised June 3, 2013

To Assign the Application Impersonation Management Role to Unified Messaging Services Accounts for Cisco Unity Connection (Office 365 Only)

Step 1   To configure impersonation in Office 365, you must run a Windows PowerShell script. For details see the, section.

Step 2   You must have the permission to run the **New-ManagementRoleAssignment** cmdlet. By default the administrators have this permission.

Use "**New-ManagementRoleAssignment**" Exchange Management Shell cmdlet to grant the service account permission to impersonate all the users in the organization.

new-ManagementRoleAssignment -Name:RoleName -Role:ApplicationImpersonation -User:Account

where:

–Name parameter specifies the name of the new role assignment, for example, ConnectionUMServicesAcct. The name that you enter for RoleName appears when you run get-ManagementRoleAssignment.

-Role parameter indicates that the ApplicationImpersonation role is assigned to the user specified by the User parameter.

–User is the name of the unified messaging services account in alias@domain format.

For example:

New-ManagementRoleAssignment –Name "ConnectionUMServicesAcct" –Role "ApplicationImpersonation" –User serviceaccount@example.onmicrosoft.com

> **Note**   This operation may not be allowed for the organization with the disabled customizations. In order to enable this operation, you need to execute the Enable-OrganizationCustomization task first, that is "*Enable-OrganizationCustomization*".

Step 3   If you created more than one unified messaging services account, repeat Step 2 for the remaining accounts. Specify a different value for RoleName for each unified messaging services account.

> **Caution**   If you have activated the Active Directory Synchronization feature and migrating from local Exchange server to Office 365, then the further user management is done through the on-premises Active Directory Services and it gets synchronized with Office 365 automatically. You must make sure the Application Impersonation Management role is given to your Office 365 server.

Accessing Office 365 Using Remote Exchange Management PowerShell

Revised October 23, 2013

To Access Office 365 Using Remote Exchange Management Power Shell

Step 1 Run Windows PowerShell as administrator and run following Command.

Set-ExecutionPolicy Unrestricted

Step 2 On a Windows PowerShell endpoint, run the following command and enter the Office-365 administrator account credentials for authentication in the popup window.

$LiveCred = Get-Credential

Step 3 To establish a remote Windows PowerShell session with Office 365, use the New-PSSession Windows PowerShell cmdlet to connect with the generic remote Windows PowerShell endpoint at http://ps.outlook.com/powershell. Run the following command to create Remote Exchange Shell Session.

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection

Note The user account you use to connect to office 365 Exchange Online must be enabled for remote shell.

Step 4 Run the following command to Import all Remote Exchange Shell Commands to the local client side session.

Import-PSSession $Session

If it fails with an error message we may need to set the Execution policy to allow running remote PowerShell scripts.Run Get-ExecutionPolicy. If the value returned is anything other than RemoteSigned, you need to change the value to RemoteSigned by running Set-ExecutionPolicy RemoteSigned

http://technet.microsoft.com/en-us/library/jj984289%28v=exchg.150%29.aspx

To use Import-PSSession, the execution policy in the current session cannot be Restricted or All signed, because the temporary module that Import-PSSession creates contains unsigned script files that are prohibited by these policies. To use Import-PSSession without changing the execution policy for the local computer, use the Scope parameter of Set-ExecutionPolicy to set a less restrictive execution policy for a single process.

http://community.office365.com/en-us/forums/158/t/71614.aspx

Creating a Unified Messaging Service to Access Office 365 from Cisco Unity Connection

Revised June 3, 2013
Do the following procedure to create one or more unified messaging services.

To Create a Unified Messaging Service to Access Office 365 from Cisco Unity Connection 8.6(2) and Later

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

Step 2 On the Search Unified Messaging Services page, select **Add New**.

Step 3 Decide which options to select for the Message Action for Email and Message Action for Fax lists at the bottom of the page. (For field information, on the Help menu, select This Page.)

If you want to select Relay the Message or Accept and Relay the Message for either list, you must first configure an SMTP Smart Host on the System Settings > SMTP Configuration > Smart Host page. Connection Administration will not let you save a new unified messaging configuration with those settings when no SMTP Smart Host is configured. For SMTP smart host server, Connection will communicate with on -premise SMTP relay servers only.

Step 4   On the New Unified Messaging Service page, in the Type list, select **Office 365**.

✎
Note   You can configure up to 1800 users with a single Office 365 Unified Messaging Service. For creating more than 1800 users with Office 365, you need to create more Unified Messaging services.

Step 5   Check the **Enabled** check box to enable the service.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes" section on page 3-5

Step 6   In the **Display Name** field, enter a descriptive name.

If you are creating more than one unified messaging service for Office 365, note that this is the name that will appear on the **Users > Unified Messaging Accounts page** when you configure users for unified messaging. Enter a display name that will simplify choosing the correct unified messaging service for each user.

Step 7   If you want Connection to validate the SSL certificate from the Exchange server, check the Validate Certificates for Exchange Servers check box.

Step 8   In the **Proxy Server** field, enter the IP Address and port in the Adress:Port or Hostname:Port format.

✎
Note   Proxy Server is an optional field that allows you to route the traffic using a Proxy server when the Office 365 network is not accessible from Connection.

Step 9   If you want Connection to automatically find Hosted Exchange client access servers, do the following:

a.   Select **Search for Hosted Exchange Servers**.

✎
Note   It is mandatory to use Search for Hosted Exchange Servers option with Office 365.

b.   Enter DNS Domain Name used for the Office 365 users.

  • In a hybrid environment where you route mails between an on-premise Exchange organization and Office 365, specify the special onmicrosoft.com domain name (such as mycompany.mail.onmicrosoft.com) provided by Microsoft.

  • If you are only using Office 365, try your domain name from your email addresses.

c.   If you have Hosted Exchange servers in more than one Active Directory site, you can improve performance if you specify the site that contains the domain controllers that you want Connection to use to find Exchange servers. In the Active Directory Site Name field, enter the name of the site.

d.   In the **Protocol Used to Communicate with Domain Controllers** list, select whether Connection should use LDAP or secure LDAP (LDAPS) when communicating with Active Directory to find Hosted Exchange servers.

⚠️

Caution   Caution: When you select Search for Hosted Exchange Servers, Connection communicates with Active Directory servers using Basic authentication. As a result, the username and password of the unified messaging services account and all other communication between the Connection and Active Directory servers is in clear text. If you want this data to be encrypted, you must select Secure LDAP (LDAPS) in the Protocol Used to Communicate with Domain Controllers list and upload certificates from the certification authority that issued the SSL certificates for Active Directory servers to both tomcat-trust and Connection-trust locations.

    e. If you want Connection to validate the SSL certificate from Active Directory domain controllers, check the **Validate Certificates for Active Directory Domain Controllers** check box.

       Self-signed certificates cannot be validated. If you selected LDAPS from the **Protocol Used to Communicate with Domain Controllers list**, and if you are using self-signed certificates, do not check the Validate Certificates for **Active Directory Domain Controllers** check box. If you do check the check box, Connection will not be able to access domain controllers to search for Hosted Exchange servers.

    f. Skip to Step 9.

Step 10   In the Username and Password fields, enter the Active Directory username and password for the Domain Service account provided by Microsoft Office 365.

       The username must be in User Principal Name(username@domain.com) format.

Step 11   Under Service Capabilities, select the features that you want this unified messaging service to allow.

✎

Note   When you configure unified messaging for Connection users, you can disable for an individual user any feature that you enable here. However, you cannot enable for an individual user any feature that you disable here.

       For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the "How Disabling and Re-enabling Single Inbox Affects the Synchronization of Connection and Office 365 Mailboxes" section on page 3-5

Step 12   Under Synchronize Connection and Office 365 Mailboxes (Single Inbox), choose message actions for email and for fax. (For field information, on the Help menu, select This Page.)

Step 13   Select **Save**

Testing Unified Messaging Services for Cisco Unity Connection

Do the following procedure to test one or more unified messaging services.

To Test Unified Messaging Services for Connection

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

Step 2   On the Search Unified Messaging Services page, select the service that you want to test.

Step 3   On the Edit Unified Messaging Service page, select **Test**.

Step 4   If the test results showed configuration problems, resolve the problems, then repeat the test.

Step 5   If you configured two or more unified messaging services, repeat Step 1 through Step 4 to test the remaining services.

Testing Unified Messaging Accounts for Cisco Unity Connection

Do the following procedure to test one or more of the unified messaging accounts that you created in the Creating the Unified Messaging Services Account on Office 365 and Granting Permissions for Cisco Unity Connection, page 3-10

To Test User Access to Office 365 for Individual Cisco Unity Connection

Step 1   In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2   On the Search Users page, select the alias of a user who is configured for one or more unified messaging features for Office 365.

> **Note**   If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

Step 3   On the Edit User Basics page, on the Edit menu, select **Unified Messaging Accounts**.

Step 4   Select a unified messaging account for Exchange.

Step 5   On the Edit Unified Messaging Account page, select **Test**.

Step 6   Review the results, resolve problems, if any, and re-run the test until no more problems are found.

Testing System Configuration, Including Unified Messaging, with Office 365 and Cisco Unity Connection

You can run a Connection system test that includes tests of the unified messaging configuration and that provides summary data on configuration problems, if any, for example, the number of accounts assigned to a specified unified messaging service that has configuration problems.

To Check System Configuration, Including Unified Messaging Configuration for Cisco Unity Connection

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

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

Step 3   Select **Run Now**.

Step 4   Select **Refresh** to display links to the latest results.

Step 5   Review the results, resolve problems, if any, and re-run the Check System Configuration task until no more problems are found.

Testing Access to Office 365 Calendars for Cisco Unity Connection

If you configured Connection access to Office 365 calendars, do the following procedure.

To Test Access to Office 365 Calendars for Cisco Unity Connection

Step 1   Sign in to Outlook.

Step 2   On the Go menu, select **Calendar**.

Step 3   On the File menu, select **New > Meeting Request**.

Step 4   Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

Step 5   Select **Send**.

Step 6   Sign in to the Cisco Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

Step 7   If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Connection reads the information about the Exchange meeting.