Configuring Cisco Unity Connection and Microsoft Office 365 for Unified Messaging

See the following sections:

Task List for Configuring 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 10.x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html#pgfId-579146.
2. Ensure you have sufficient licenses for voicemail users:
   a. Navigate to Cisco Unity Connection Administration, expand **System Settings** and select **Licenses**.
   b. On the Licenses page, in the **License Usage** section, check **Total number of Voicemail Users**.
3. *If Unity Connection is integrated with an LDAP directory:* Navigate to Cisco Unity Connection Administration and make sure of the following:
   - Expand **System Settings** and select **LDAP Directory Configuration**. Select the applicable LDAP directory configuration. On the LDAP Directory Configuration page, make sure the **Mail ID** field in **Cisco Unified Communications Manager User Fields** is synchronized with the **mail** in **LDAP Attribute**.

   This causes values in the **LDAP mail** field to appear in the **Corporate Email Address** field in an LDAP imported user.

Note For more information, see the "LDAP" chapter in the *System Administration Guide for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx/10xcucsag120.html.

- Expand **Users** and select **Users**. Select the applicable user. On the Edit User Basics page, value in the **Corporate Email Address** field is specified.

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 for latest releases,* 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 Unity Connection and Office 365 server. For more information, refer to "Latency" section of the “Single Inbox in Cisco Unity Connection 10.x” chapter in the *Design Guide for Cisco Unity Connection*, *Release 10.x*, available at:

   http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx/10xcucdg032.html#pgfId-1132131.
6. Select search for and communicate with different Office 365 server**. 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 Unity 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 Unity Connection unified messaging services, and grant the account the applicable permissions. See the Configuring Unity Connection and Office 365 for Unified Messaging, page 3-5 section.
8. Update the settings for Unity Connection users. For more information, see the Settings Configured on Unity Connection Users, page 2-22 section.
9. Configure one or more Unity Connection unified messaging services. See the Creating a Unified Messaging Service to Access Office 365, page 3-6 section.
10. *Selected configurations:* For the following configuration, upload SSL certificates on the Unity Connection server to encrypt communication between Unity Connection and Office 365 and between Unity 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.

Caution When you allow Unity Connection to search for and communicate with Office 365 servers, Unity 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 Unity Connection and Active Directory servers is sent in clear text. If you want this data to be encrypted, in Task 9. you must configure unified messaging services to communicate with Active Directory domain controllers using the secure LDAP (LDAPS) protocol.

For more information, see the Uploading CA Public Certificates for Exchange and Active Directory Servers to Unity Connection, page 2-23 and Uploading Certificates for Office 365 and Cisco Unity Connection, page 2-25 section.

11. Test the unified messaging configuration. For more information, see the Testing Unified Messaging Configuration, page 3-6 section.
12. *If Unity 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**.
13. To teach users how to use the Unity Connection calendar, refer them to the following:
    - For listing, joining, and scheduling meetings, see the "Working With Cisco Unity Connection By Phone" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/user/guide/phone/b_10xcucugphone/b_10xcucugphone_chapter_01.html.
    - For importing Exchange contacts, see the "Managing Your Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst/b_10xcucugasst_chapter_01001.html.
    - For using personal call transfer rules, see the "*Personal Call Transfer Rules Web Tool"* at *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/user/guide/pctr/b_10xcucugpctr/b_10xcucugpctr_chapter_00.html.

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

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

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

Follow the given steps to create a unified messaging services account and grant permissions:

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 create a Office 365 mailbox for the account.
    - 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 Assigning the Application Impersonation Management Role to Unified Messaging Services Accounts (Office 365 only), page 3-4.

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

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

Step 1 To configure impersonation in Office 365, you must run a Windows PowerShell script. For details see the, "Accessing Office 365 Using Remote Exchange Management PowerShell" section on page 3-5 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

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

To Access Office 365 Using Remote Exchange Management Power Shell

Step 1 Run Windows PowerShell as administrator and run the 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 signe**d, 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.

Configuring Unity Connection and Office 365 for Unified Messaging

See the following sections:

- Creating Unified Messaging Services Account on Office 365 and Granting Permissions for Unity Connection, page 3-3
- Creating a Unified Messaging Service to Access Office 365, page 3-6
- Testing Unified Messaging Configuration, page 3-6

Creating a Unified Messaging Service to Access Office 365

To Create a Unified Messaging Service to Access Office 365

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

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

Step 3 On the New Unified Messaging Service page, in the **Type** list, select **Office 365** and check the **Enabled** check box. Enter the values of the required fields. (For more information on each field, see **Help> This Page**).

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.

For information on synchronization behavior if you later disable a unified messaging service for which single inbox is enabled, see the Disabling and Re-enabling Single Inbox Affects the Synchronization of Unity Connection and Exchange/ Office 365 Mailboxes, page 1-8 section.

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

Caution Caution: When you select **Search for Hosted Exchange Servers**, Unity 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.

Step 4 Under **Service Capabilities**, select the features that you want this unified messaging service to allow.

Note When you configure unified messaging for Unity 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.

Step 5 Under **Synchronize Connection and Office 365 Mailboxes (Single Inbox)**, select message actions for email and for fax and select **Save**.

Testing Unified Messaging Configuration

See the following sections:

- Testing Unified Messaging Services, page 3-7
- Testing Unified Messaging Accounts, page 3-7

Testing Unified Messaging Services

To Test Unified Messaging Services

Step 1 In Cisco Unity Connection Administration, expand **Unified Messaging** and select **Unified Messaging Services**. On the Search Unified Messaging Services page, select the service that you want to test.

Step 2 On the Edit Unified Messaging Service page, select **Test**.

Step 3 If the test results showed configuration problems, resolve the problems, then repeat the test.

Step 4 If you configured two or more unified messaging services, repeat Step 1 through Step 3 to test the remaining services.

Testing Unified Messaging Accounts

Do the following procedure to test one or more of the unified messaging accounts that you created in the Configuring Unity Connection and Office 365 for Unified Messaging, page 3-5

To Test User Access to Office 365 for Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select the alias of a user who is configured for one or more unified messaging features for Office 365.

Step 2 On the Edit User Basics page, on the **Edit** menu, select **Unified Messaging Accounts**. Select a unified messaging account for Exchange.

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

Step 4 Review the results, resolve problems, if any, and re-run the test until no more problems are found.

Testing System Configuration and Unified Messaging with Office 365 and Unity Connection

You can run a Unity 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 Unity Connection

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

Step 2 On the Task Definitions page, select **Check System Configuration** and then select **Run Now**.

Step 3 Select **Refresh** to display links to the latest results.

Step 4 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

To Test Access to Office 365 Calendars for 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 Unity Connection.

Step 5 Select **Send**.

Step 6 Sign in to the 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.

Unity Connection reads the information about the Exchange meeting.