# Configuring Unified Messaging

Cisco Unity Connection can be integrated with Microsoft Exchange 2019, 2016, Office 365 and Gmail Server to deploy the unified messaging feature.



# Overview of Unity Connection Communication with Exchange Server

When you add a unified messaging service that defines the communication between Unity Connection and Exchange, you can select whether you want Unity Connection to communicate directly with a specific Exchange server or you want Unity Connection to search for Exchange servers.

The choice you make determines which Exchange mailboxes Unity Connection can access:

- If you select a specific Exchange 2016 client access server, Unity Connection can access all Exchange 2016 mailboxes in the Exchange organization, but cannot access Exchange 2019 mailboxes.
- If you select a specific Exchange 2019 client access server, Unity Connection can access all Exchange 2019, and Exchange 2016 mailboxes in the Exchange organization.
- If you allow Unity Connection to search for Exchange servers, you need to give permissions to the Exchange servers. See the below section to grant permissions to the applicable Exchange server:

Granting Permissions for Exchange 2016 or Exchange 2019, on page 12

**Note** If you want to select a specific Exchange server when you add a unified messaging service, you may need to add more than one unified messaging service to allow Unity Connection to access all mailboxes in the Exchange organization. Table 1 explains when you need to add more than one unified messaging service.

*Table 1: Adding Unified Messaging Services Based on Versions of Exchange*

| Exchange Versions with Mailboxes That You Want Unity Connection to be Able to Access | | | |
|---|---|---|---|
| Exchange 2016 | Exchange 2019 | Office 365 | Create the Following Unified Messaging Services |
| No | No | Yes | One for Office 365 server that you want Unity Connection to be able to access. |
| No | Yes | Yes | • One for Exchange 2019.<br>• One for Office 365 server that you want Unity Connection to be able to access. |
| Yes | Yes | Yes | • One for Exchange 2019. This service can also access Exchange 2016 mailboxes.<br>• One for Office 365 server that you want Unity Connection to be able to access. |
| Yes | Yes | Yes | • One for Exchange 2019. This service can also access Exchange 2016 mailboxes.<br>• One for Office 365 server that you want Unity Connection to be able to access. |
| Yes | No | Yes | • One for Exchange 2016.<br>• One for Office 365 server that you want Unity Connection to be able to access. |
| Yes | No | No | One for Exchange 2016. |

| Exchange Versions with Mailboxes That You Want Unity Connection to be Able to Access | | | |
|---|---|---|---|
| Yes | No | Yes | • One for Exchange 2016.<br>• One for Office 365 server that you want Unity Connection to be able to access. |
| No | No | Yes | • One for Office 365 server that you want Unity Connection to be able to access. |

- If you select to allow Unity Connection to search for Exchange servers, Unity Connection automatically detects when you move mailboxes from one version of Exchange to another, and automatically update Unity Connection user settings.
- If you select a specific Exchange server, Unity Connection sometimes detects when you move mailboxes from one Exchange server to another, and automatically access the Exchange mailbox in new location. When Unity Connection cannot detect the new mailbox, you must manually update unified messaging services or unified messaging accounts:
  - *If you moved all the Exchange mailboxes accessed by a unified messaging service:* Update the unified messaging service to access a different Exchange server.
  - *If you moved only some of the Exchange mailboxes accessed by a unified messaging service:* Update unified messaging account settings to use a unified messaging service that accesses mailboxes in the new location.

Table 2 identifies when Unity Connection automatically detect mailbox moves between Exchange servers. For information on updating Unity Connection user settings when Unity Connection cannot detect mailbox moves, see the "Moving and Restoring Exchange Mailboxes" chapter.

***Table 2: Choosing a Specific Exchange Server: When Unity Connection Detect Moving a Mailbox Between Exchange Servers***

| If you select a specific | Unity Connection can automatically detect mailbox moves between the following Exchange versions | | | | |
|---|---|---|---|---|---|
| | **2016** | **2019** | **2016 and 2016** | **2016 and 2019** | **2019 and 2019** |
| Exchange 2016 server | Yes | No | Yes | No | No |
| Exchange 2019 server | Yes | Yes | Yes | Yes | Yes |

If Unity Connection is not configured to use DNS, you must select a specific Exchange server. If this does not allow you to access all the Exchange mailboxes in the organization as described earlier in this section, you must create more than one unified messaging service.

If you select a specific Exchange server and that server stops functioning, Unity Connection cannot access any Exchange mailboxes. If you select to allow Unity Connection to search for Exchange servers and if the Exchange server that Unity Connection is currently communicating with stops functioning, Unity Connection searches for another Exchange server and begins accessing mailboxes through that server.

# Unified Messaging with Google Workspace

Unity Connection 15 and later provides user a new way to access the emails and voice messages on the Gmail account of the user. It allows administrator to integrate unified messaging with Google Workspace. Using Google Workspace, you can configure Unity Connection to synchronize voice messages between Unity Connection and Gmail Server. All Unity Connection voice messages that are sent to user, are first stored in Unity Connection and then synchronized to the user's Gmail account.

# Prerequisites for Configuring Unified Messaging

Following prerequisites should be met before configuring Unified Messaging:

1. Review the "Requirements for Using Unified Messaging Features" section in the System Requirements for Cisco Unity Connection Release 15, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html
2. If *Unity Connection is integrated with an LDAP directory* : Navigate to Cisco Unity Connection Administration and verify 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 of the LDAP imported user.
   - Expand **Users** and select **Users**. Select the applicable user. On the Edit User Basics page, enter the **Corporate Email Address**.
   - Select **Edit** on the user page and then select **Unified Messaging Account**. On the Unified Messaging Account page of the user, make sure value in the **Email Address** field is specified.

# Task List for Configuring Unified Messaging

## Task List for Configuring Unified Messaging with Exchange 2016 or Exchange 2019

**Step 1** Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

**Step 2** Create an Active Directory account for unified messaging users to communicate with Exchange 2016 or Exchange 2019. For more information on creating unified messaging services account in Active Directory and granting permissions, see the Configuring Unified Messaging in Active Directory section.

**Step 3** Decide whether you want Unity Connection to be able to search for and communicate with different Exchange 2016 or Exchange 2019 server, or you want Unity Connection to communicate with a specific Exchange 2016 or Exchange 2019 server in case the hostname or the IP Address of the specific server is known. Do the following steps:

a) Granting Permissions for Exchange 2016 or Exchange 2019, on page 12

b) *(Optional)* Confirming Exchange 2016 or Exchange 2019 Authentication and SSL Settings, on page 13

**Note** Unity Connection determines whether to use the HTTP or HTTPS protocol and whether to validate certificates based on settings specified in the associated unified messaging service.

**Step 4** If Unity Connection is not configured to use DNS, use the following CLI commands to configure DNS:

- **set network dns**
- **set network dns options**

**Note** 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.

**Step 5** *(Selected configurations only)*: In either or both of the following conditions, you need to upload SSL certificates on the Unity Connection server to encrypt communication between Unity Connection and Exchange and between Unity Connection and Active Directory:

- If you have configured Exchange to use HTTPS in Step 3 b, configure unified messaging services to validate certificates for Exchange servers.
- If you have configured Unity 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 different Exchange servers, Unity Connection communicates with Active Directory servers using Basic authentication. By default, the username 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, 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 section.

**Step 6** Configure one or more unified messaging services on Unity Connection. For more information, see theGranting Permissions section.

**Step 7** Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

**Step 8** Configure one or more unified messaging accounts to link the Unity Connection users with the mail server with which they are communicating. For more information, see the Unified Messaging Account for Users section.

**Step 9** Test unified messaging configuration. For more information, see the Test Unified Messaging Configuration section.

# Task List for Configuring Unified Messaging with Office 365

**Step 1** Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

**Step 2** Create an Active Directory account to be used by Unity Connection unified messaging users to communicate with Office 365. For more information on creating unified messaging services account in Active Directory and granting permissions, see the Configuring Unified Messaging in Active Directory section.

**Step 3** Decide and select the type of authentication that you want Unity Connection to use to sign in to Office 365 client access servers. To do this, navigate to **Unified Messaging** > **Unified Messaging Services** on Cisco Unity Connection Administration and select **Add New**. On the New Unified Messaging Service page, select either of the following from **Web-Based Authentication Mode** field:

- **Basic**: Default authentication mode.
- **NTLM**: Before switching to NTLM authentication mode, make sure that the same mode is configured on the Office 365 server.
- **OAuth2** : OAuth 2.0 based authentication mode.

**Note** Basic authentication has been deprecated by Microsoft

Cisco Unity Connection supports **OAuth2** authentication mode for configuring Unified Messaging with Office 365. For using OAuth2 web authentication mode, you must create and register an application on Microsoft Azure portal corresponding to the Unified Messaging Service. For more information, see Step 4.

For existing Unified Messaging Service, select the above settings on Edit Unified Messaging Service page.

**Step 4** *(Applicable only for OAuth2 web authentication mode)* Refer the following steps for registering the application on Azure portal.

**Note** The steps may be changed or modified as per the latest updates available from Microsoft.

a) Sign in to Azure portal global endpoint at portal.azure.com with Azure portal Administrator to create Unified Messaging Service account. For other applicable Azure portal endpoints, refer section **App registration endpoints** in microsoft documentation available at link https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud

b) On the portal, select **Azure Active Directory**. A new window of Azure Active Directory appears.

c) On Azure Active Directory window, select **App registrations** and create a new application using **New registration** field. After successfully registering the application, you get the values of **Application (Client) ID** and **Directory ID** that are used for configuring Unified Messaging.

d) Select **Certificates & secrets** and create a new **Client Secret** that provides a Client Secret value, used for configuring Unified Messaging.

**Note** Make sure to copy the value of Client secret at the time of creation otherwise you have to create a new Client Secret for the application.

e) Select **API permissions** > **Add a permission** > **APIs my organization uses**. Enter **Office 365 Exchange Online** in search bar and select it.

f) *(Applicable to 14SU2 and earlier releases)* Click **Delegated permissions** and add below permissions in your application:

| Features | Permissions |
|---|---|
| EWS | EWS.AccessAsUser.All |

| Features | Permissions |
|---|---|
| Mail | Mail.ReadWrite, Mail.Send |

For accessing Calendar and Contacts, you should also add below permissions in your application:

| Features | Permissions |
|---|---|
| Calendars | Calendars.ReadWrite |
| Contacts | Contacts.ReadWrite |

g) *(Applicable to 14SU3 and later releases)* Click **Application permissions** and add **full_access_as_app** permission in your application. To restrict the permissions, see steps mentioned inTask List for restricting Application Permissions to mailboxes, on page 9.

h) On API permissions window, select **Grant admin consent for <Directory/Tenant Name>** to provide grant admin consent for the requested permissions.

For more information on registering Application on Azure portal, see https://docs.microsoft.com/en-us/graph/auth-register-app-v2.

**Step 5** *(Applicable only for OAuth2 web authentication mode)* Enter the values of below fields getting from the Azure portal in step 4:

- **Application (Client) ID.**
- **Directory ID.**
- **Client Secret.**
- **AD Authentication Endpoint.** Its default value is https://login.microsoftonline.com.

  **Note** For other applicable AD Authentication Endpoints refer section **Azure AD authentication endpoints** in Microsoft documentation available at link https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud

- **Resource URI.** Its default value is https://outlook.office365.com.

**Note** Repeat Steps 4 and 5 for the following:

- In case of multiple clusters , the above fields should be unique for each cluster configuration.
- When configuring multiple Unified Messaging services in Unity Connection you must create a unique Client ID for each service.

**Step 6** *(Applicable to 14SU2 and earlier releases)* Do the following tasks on the Office 365 server to enable Auto Discovery functionality that enables Unity Connection to search for and communicate with different Office 365 servers:

a) Accessing Office 365 Using Remote Exchange Management Power Shell

b) (Applicable for 14SU2 and earlier releases) Assigning Application Impersonation Role for Office 365

**Note** Unity Connection uses the HTTPS protocol to validate certificates based on the settings in the applicable unified messaging service.

**Step 7** Synchronization threads configuration should be done based on latency between Unity Connection and Office 365 server. For more information, see the "Latency" section of the “Single Inbox” chapter in the *Design Guide for Cisco Unity Connection Release 15*, available at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/guide/b_15cucdg.html

**Step 8** Run the following CLI commands to configure DNS:

- **set network dns**
- **set network dns options**

**Note** 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.

**Step 9** (*Selected configurations only*): Upload SSL certificates on the Unity Connection server to encrypt the communication between Unity Connection and Office 365. Uploading certificates allows you to:

- Validate the certificates for Exchange Servers. To do this, check the **Validate Certificates for Exchange Servers** check box on Unity Connection Administration.
- Secure communication when you have configured Unity Connection to search for and communicate with Office 365 servers.

For more information, see the Uploading the Public Certificates to the Unity Connection Server and Uploading Certificates for Office 365 and Cisco Unity Connection

**Step 10** Create one **Unified Messaging Service** and configure all the users with that service account.

**Note** If Unity Connection server is being shared by tenants for voicemail service, then multiple **Unified Messaging Service** accounts are required.

**Step 11** Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

**Step 12** Run the following CLI commands to configure the number of users aggregated per streaming thread and hourly periodic full resynchronization flag for mailbox synch.

a) Check the existing number of users.

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchUserCountPerStreamingSubscription'
```

If "value" parameter is 5000, it means configuration is already enabled. If value is not 5000, run the below CLI command to set the number of users.

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyLong(pFullName='System.Messaging.MbxSynch.MbxSynchUserCountPerStreamingSubscription',pvalue=5000)
```

b) Check the existing configuration of the hourly periodic full resynchronization flag for mailbox synch.

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchBackgroundSyncEnable'
```

If "value" parameter is 0, it means the configuration is already enabled.If value is not 0, run the below CLI command to set the flag.

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchBackgroundSyncEnable',pvalue=0)
```

c) You must restart **Connection Mailbox Sync** service for above CLI changes to come into effect.

**Note** In case of cluster, execute the commands only on publisher server and after that make sure that database replication is working fine.

**Step 13** Test the unified messaging service. For more information, see the Test Unified Messaging Configuration

## Task List for restricting Application Permissions to mailboxes

**Step 1** Create a **mail-enabled security group**. It can be used to distribute messages and to grant access permissions to resources in Active Directory. See steps available at https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-mail-enabled-security-groups#use-the-exchange-admin-center-to-manage-a-mail-enabled-security-group.

**Step 2** Install the **Exchange Online Management Module** in an elevated Powershell. See steps available at https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exchange-online-powershell-module.

**Step 3** Connect to **Exchange Online PowerShell**. See steps available at https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps.

**Step 4** Run the **New-ApplicationAccessPolicy** cmdlet. For running New-ApplicationPolicy, **OrganizationConfiguration** Role is required. You can check the current Role by the following command:

```
Get-ManagementRole -Cmdlet <Cmdlet>
```

Do the following steps for assigning OrganizationConfiguration role to the admin user :

a) Login Exchange Admin Center at https://admin.exchange.microsoft.com/.
b) Select **Roles → Admin Roles**.
c) Select **Organization Management** role for the user.
d) Restart Power Shell to make sure the new role assignment is in effect

**Step 5** Run the **New-ApplicationAccessPolicy** cmdlet by the following command:.

```
New-ApplicationAccessPolicy -AppId "**" -PolicyScopeGroupId "**" -AccessRight RestrictAccess
-Description "Restrict this app to members."
```

**Note** AppId is the Application Id of the Application for which you want to restrict the access. It will be the client id mentioned in Azure Active Directory Portal for the application. You can also provide multiple appid's separated by commas. PolicyScopeGroupId is Id to identify the group. It will be the Mail enabled security group mentioned in **Step 1**.

**Note** The steps may be changed or modified as per the latest updates available from Microsoft.

# Task List for Configuring Unified Messaging with Google Workspace

Gmail API provides server push notifications through which, user examine the changes in user mailbox on Gmail server. Whenever there is a change in user mailbox, Gmail API sends notification to Unity Connection.

**Step 1** Make sure that you have met the prerequisites before configuring unified messaging. See the Prerequisites for Configuring Unified Messaging section.

Before configuring unified messaging with Google Workspace, you must have domain name to create an account on Google Workspace.

**Step 2** Go to Google Workspace and create an account on Admin Console using domain name. For detailed step, see https://workspace.google.com/signup/businessstarter/welcome?hl=en-IN.

**Step 3** Go to Google Cloud Platform (GCP) Console and login to Google Cloud Console with administrator account created in Step 2 and create a new Project.

The project specifies the domain that is used to create a service account.

**Step 4** On Google Cloud Platform, to create a new project, select **NEW PROJECT** option from the drop-down menu of the organization domain and enter the required information and select **CREATE**.

**Step 5** After creating the project, select your project from the drop-down menu of the organization domain.

**Step 6** On the project home page, navigate Menu > IAM & Admin > Service accounts > Create service account.

**Step 7** On Create Service Account page, enter the required information and select **CREATE AND CONTINUE**.

**Step 8** To provide all the permissions to the sevice account, select **Owner** role from the drop-down menu of **Role** under **Grant this sevice account access to project** field.

**Step 9** Select **DONE**.

A new page opens with all sevice accounts created under the project.

**Step 10** Select the service account created in Step 7.

**Step 11** On the sevice account page, go to **DETAILS** tab and select **SHOW DOMAIN-WIDE DELEGATION** field and check the **Enable Google Workspace Domain-wide Delegation** check box to allow service account to access all users data on a Google Workspace domain.

**Step 12** Select **SAVE**.

**Step 13** On the sevice account page, go to **KEYS** tab and select **ADD KEY** > **Create new key**.

Make sure to select JSON option in **Key type** field.

After successfully created the account, key file in .json format is downloaded on the system. The key file is used for configuring unified messaging with Google Workspace.

**Step 14** Navigate to **Menu** > **API & Services** > **Library** and search for Gmail API and enable it.

Similarly, search for Cloud Pub/Sub API and enable it.

**Step 15** To delegate domain-wide authority to Service Account, navigate Menu > IAM & Admin > Service accounts and select **View Client ID** corresponding to the service account created and copy the Client ID.

**Step 16** Log in to Admin Console and navigate Menu > Security > API controls.

**Step 17** On API controls page, select Domain-wide Delegation and select Add new.

**Step 18** A new window appears to enter the client ID.

**Step 19** On Add a new client ID window, enter the Client ID copied in Step 15 and provide OAuth scopes and select AUTHORIZE.

Scopes required :

https://mail.google.com,

https://www.googleapis.com/auth/gmail.labels,

https://www.googleapis.com/auth/gmail.modify,

https://www.googleapis.com/auth/cloud-platform,

https://www.googleapis.com/auth/pubsub

**Step 20** Create users using **Users** application on Admin Console.

**Step 21** Login to Cisco Unity Connection Administration, navigate to **Unified Messaging** > **Unified Messaging Services** and select **Add New**.

**Step 22** On the New Unified Messaging Service page, select Google Workspace for New Unified Messaging Service.

**Step 23** To enable Unified Messaging with Google Workspace feature, check **Enabled** check box.

By default the check box is checked.

**Step 24** To enable verification of Google Workspace Certificates , check **Validate Certificates for Google Workspace** check box.

By default the check box is unchecked.

**Step 25** Enter display name for new unified messaging service.

**Step 26** Enter **Proxy Server (Address:Port)** field for proxy server if required.

**Step 27** Check **Enable Proxy Server Authentication** check box to enable proxy server based authentication and provide the **Username** and **Password** for the proxy server.

**Step 28** In, **Google Workspace Service Account Key File**, upload key file created in Step 13.

Make sure to upload the file in .json format and its size should be less than 1MB.

**Step 29** Select Save.

**Step 30** Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

**Step 31** Configure one or more unified messaging accounts to link the Unity Connection users with the mail server with which they are communicating. For more information, see the Unified Messaging Account for Users section.

# Task for Configuring Unified Messaging

## Configuring Unified Messaging in Active Directory

Unity Connection accesses mailboxes on configured mail servers using an Active Directory account called the unified messaging services account. After account creation, administrator can grant it rights necessary for Unity Connection to perform operations on behalf of user.

For Office 365, Exchange 2019, Exchange 2016 following operations are performed through Exchange Web Services (EWS).

- Tracking changes to messages in Exchange
- Updating messages with changes made in Unity Connection
- Deleting messages in Exchange when the messages are deleted in Unity Connection, and so on.

- Uploading messages into Exchange mailbox.

For Gmail server following operations are performed through Gmail API.

- Synchronization of messages between Unity Connection and user's mailbox.
- Synchronization of message status like[read/unread] between Unity Connection and user's mailbox.
- Message operations like update/delete synchronization between Unity Connection and user's mailbox.

You need to create one or more domain user accounts in the Active Directory forest that includes the servers with which you want Unity Connection to communicate. Note the following points while configuring Unified Messaging in active directory:

- Give the account a name that identifies it as the unified messaging services account for Unity Connection.
- Do not create a mailbox for the domain user account. If you create a mailbox for the account, unified messaging does not function properly.

**Caution** Some newer Exchange versions need mailbox for domain user account.You need to create a mailbox for domain user account if you face any issue while testing Unified Messaging Service/Account.

- Do not add the account to any administrator group.
- Do not disable the account or Unity Connection cannot use it to access mailbox on server side.
- Specify a password that satisfies the password-security requirements.
- When administrator is configuring unified messaging for a cluster, Unity Connection automatically uses the same unified messaging services account for both Unity Connection servers.
- When administrator is configuring unified messaging for intersite networking or for intrasite networking, then same unified messaging services account can be used for more than one Unity Connection servers. However, this is not a requirement and does not affect functionality or performance.

# Granting Permissions

## Granting Permissions for Exchange 2016 or Exchange 2019

**Step 1** Sign in to a server on which Exchange Management Shell is installed using either an account that is a member of the Enterprise Admins group or an account that can grant permissions on Exchange objects in the configuration container.

**Step 2** Run the following command in Exchange Management Shell to assign the Application Impersonation management role to the unified messaging services account for Exchange 2016 or Exchange 2019:

**New-ManagementRoleAssignment -Name:** <RoleName> **-Role:ApplicationImpersonation -User:**' <Account> ', where:

- *RoleName* is the name that you want to give the assignment, for example, Unity ConnectionUMServicesAcct. The name that you enter for *RoleName* appears when you run get-ManagementRoleAssignment.
- *Account* is the name of the unified messaging services account in domain\alias format.

If you have 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.

**Note** When configuring unified messaging service account for Exchange 2016 or Exchange 2019 you need to assign the Application Impersonation management role to the unified messaging service account.

# Confirming Authentication and SSL Settings

After choosing the Exchange server accessed by Unity Connection for unified messaging, confirm that the Exchange servers are configured to use the desired authentication mode (Basic, Digest, or NTLM) and web-based protocol (HTTPS or HTTP).

Unity Connection supports NTLMv2 based authentication when a user selects NTLM authentication mode for configuring unified messaging.

After configuring the authentication mode and web-based protocols on Exchange servers, create one or more Unity Connection unified messaging services. Select the same authentication mode and web-based protocol that you specify in the servers.

## Confirming Exchange 2016 or Exchange 2019 Authentication and SSL Settings

**Step 1** Decide the type of authentication (**Basic** or **NTLM**) you want Unity Connection to use to sign in to Exchange 2016 or Exchange 2019 client access servers. You must configure all Exchange 2016 or Exchange 2019 client access servers to use the same type of authentication.

**Step 2** Decide whether you want the communication between Unity Connection and Exchange 2016 or Exchange 2019 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on all the Exchange 2016 or Exchange 2019 client access servers.

**Step 3** Sign in to a server that has access to the same Exchange 2016 client servers that is accessed by the Unity Connection. Use an account that is a member of the Local Administrators group.

**Step 4** On the Windows Start menu, select **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

**Step 5** For the first Exchange 2016 or Exchange 2019 client access server for which you want to confirm settings, in the left pane, expand <servername> > **Sites** > **Default Website**>. You need to verify the authentication settings for both EWS and Autodiscover.

**Step 6** Under **Default Website**, select **Autodiscover**:

a) In the middle pane, in the **IIS** section, double-click **Authentication**.

Confirm that the Status column says **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange client access servers.

When you create a unified messaging services account, you configure Unity Connection to use the same type of authentication. Unity Connection supports only the following types of authentication:

- **Basic**
- **NTLM**

b) If you have changed any settings, in the right pane, select **Apply**.

c) In the left pane, select **Autodiscover** again.

d) In the middle pane, double-click **SSL Settings**.
e) On the SSL Settings page, if the **Require SSL** check box is checked:
   - You must select HTTPS for the web-based protocol while creating a unified messaging service in Unity Connection.
   - You must download SSL certificates from the Exchange server and install them on the Unity Connection server.
f) If you changed any settings, in the right pane, select **Apply**.

**Step 7** Under **Default Website**, select **EWS**:
a) In the middle pane, in the IIS section, double-click **Authentication**.

   Confirm that the **Status** column displays **Enabled** for the type of authentication that you want the unified messaging services account to use to sign in to Exchange mailboxes. When you create a unified messaging services account, you configure Unity Connection to use the same type of authentication.

   **Caution** The unified messaging services account must use the same type of authentication for EWS that you specified for autodiscover.

b) If you changed any settings, in the right pane, select **Apply**.
c) In the left pane, select **EWS** again.
d) In the middle pane, double-click **SSL Settings**.
e) If the **Require SSL** check box is checked:
   - You must select HTTPS for the web-based protocol when you create a unified messaging service in Unity Connection.
   - You must download SSL certificates from the Exchange server and install them on the Unity Connection server.

   **Caution** The unified messaging services account must use the same SSL settings for EWS that you specified for autodiscover in Step e.

f) If you have changed any settings, in the right pane, select **Apply**.

**Step 8** Repeat Step 5 through Step 6 for the other Exchange 2016 or Exchange 2019 client access servers that Unity Connection can access.

**Step 9** Close **IIS Manager**.

# Configuring Paged View Functionality in Unity Connection for Exchange 2016 or Exchange 2019

If any unified user Exchange mailboxes have more than 1000 messages including voicemails and receipts, then enable the EWS paged view search functionality in Unity Connection server.

To enable the paged view functionality for messages, you must set the value of the 'System.Messaging.MbxSynch.MbxSynchUsePaging' parameter to 1.

Do the following to configure paged view functionality:

**Step 1** Run the following CLI command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchUsePaging',pvalue=1)
```

**Note** When a Unity Connection cluster is configured, you can run the command on publisher or subscriber server.

**Step 2** To set the maximum limit of voicemails items that can be managed by Unity Connection with the Paged view search functionality, run the following CLI command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pFullName='System.Messaging.MbxSynch.MbxSynchVoiceMailCountLimit',pvalue="newvalue")
```

where new value specifies the value of the voicemails count limit that you can view after the paging parameter is enabled. Unity Connection by default manages the first 25000 voicemails per mailbox which avoids any delay in message synchronization between Unity Connection and Exchange server. This voicemail count limit can be increased maximum up to 75000.

**Note** By default, the value of the parameter ‘System.Messaging.MbxSynch.MbxSynchUsePaging' parameter is set to 1.

# Accessing 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 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.

# (*Applicable for 14SU2 and earlier releases)* Assigning Application Impersonation Role for Office 365

**Step 1** To configure impersonation in Office 365, you must run a Windows PowerShell script.

**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**

**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.

# Creating a Unified Messaging Service to Access Mail Server

Do the following procedure to create one or more unified messaging services in Unity Connection to access the supported mail server.

**Note** If you configured the supported mail server to use HTTPS, you need to configure the unified messaging services to validate certificates for the mail servers. You need to upload certificates from the certification authority that issued the SSL certificates for mail server to both Tomcat-trust and Unity Connection-trust locations. For information on uploading SSL certificates, see the "Using SSL to Secure Client/Server Connections" chapter of the *Security Guide for Cisco Unity Connection Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/guide/b_15cucsecx.html.

## Creating Unified Messaging Services in Unity Connection

If you are configuring Unity Connection to communicate with individual mail servers, you need to configure unified messaging services for each mail server.

**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** to create a new unified messaging services. You may also select an already created unified messaging services and modify its settings. The New Unified Messaging Services page or Edit Unified Messaging services page appears.

**Step 3** Enter the values of the required fields to configure unified messaging services and select **Save** (For information on each field, see **Help> This Page** depending on the mail server you selected).

If you are configuring Unity Connection to communicate with individual mail servers, you need to configure unified messaging services for each mail server.

# Uploading CA Public Certificates for Exchange and Active Directory

At the time of creating unified messaging services, if you selected to validate certificates for Exchange servers or for Active Directory domain controllers (DCs), you must upload the public certificates from the certification authority (CA) that signed the certificates on the Exchange servers and DCs.

The public certificates allow Unity Connection to communicate with Exchange servers or DCs and unified messaging functions properly.

1. *If you selected the option to validate certificates for Exchange servers, and if SSL certificates are not already installed on all of the following servers:* Get and install certificates:

   - Exchange 2019 or Exchange 2016 client access servers.

   In addition, if you selected the option to validate certificates for Active Directory domain controllers, and if SSL certificates are not already installed on your DCs, get and install certificates.

2. *If you used an external CA (for example, Verisign) to issue the SSL certificates installed on the servers listed, and if you have the public certificates for the CA in .pem format:* Save the files to a network location accessible to the Unity Connection server. Then skip to Task 6.

3. *If you used Microsoft Certificate Services or Active Directory Certificate Services to issue the SSL certificates, or if you used an external CA and you do not have the public certificate for the CA in .pem format:* Download and install OpenSSL or another application that can convert public certificates to .pem format. Unity Connection cannot upload public certificates in other formats.

4. *If you used Microsoft Certificate Services to issue the SSL certificates:* Do the Saving the Public Certificate for Microsoft Certificate Services or Active Directory Certificate Services to a File.

5. *If you used Microsoft Certificate Services, Active Directory Certificate Services, or an external CA, and if you do not have public certificates in .pem format:* Use the application that you have downloaded to convert the public certificate to .pem format, and save the file to a network location accessible to the Unity Connection server.

6. Upload the public certificates to the Unity Connection server. For more information, see the Uploading the Public Certificates to the Unity Connection Server. and Uploading Certificates for Office 365 and Cisco Unity Connection

## Saving the Public Certificate for Microsoft Certificate Services or Active Directory Certificate Services to a File

**Step 1** Sign in to the server on which you installed Microsoft Certificate Services and issued SSL certificates for the following servers:

- Exchange 2019 or Exchange 2016 client access servers.
- Active Directory domain controllers that the Unity Connection server might access.

**Step 2** On the Windows Start menu, select **Programs** > **Administrative Tools** > **Certification Authority**.

**Step 3** In the left pane of the **Certification Authority MMC**, right-click the server name, and select **Properties**.

**Step 4** In the <*servername*> **Properties** dialog box, on the General tab, select **View Certificate**.

**Step 5** In the **Certificate** dialog box, select the **Details** tab.

**Step 6** On the **Details** tab, select **Copy to File**.

**Step 7** On the Welcome to the Certificate Export Wizard page, select **Next**.

**Step 8** On the Export File Format page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.

**Step 9** On the File to Export page, specify the full path of the public certificate, including a location that is accessible to the Unity Connection server, and a file name.

**Step 10** Select **Next**.

**Step 11** On the Completing the Certificate Export Wizard page, select **Finish**.

**Step 12** Select **OK** three times to close a message box and two dialog boxes.

**Step 13** Close the **Certification Authority MMC**.

**Step 14** If you issued SSL certificates for all of the servers listed in Step 1 using the same installation of Microsoft Certificate Services, you are finished with this procedure. Return to the task list for this section.

If you issued SSL certificates for all of the servers listed in Step 1 using different installations of Microsoft Certificate Services, repeat Step 1 through Step 13 to get one public certificate for each instance of Microsoft Certificate Services. Then return to the task list for this section.

## Uploading the Public Certificates to the Unity Connection Server

**Step 1** In Cisco Unified Operating System Administration, expand Security and select **Certificate Management**.

**Step 2** On the Certificate Management page, select **Upload Certificate**.

**Step 3** In the Certificate Name list, select **tomcat-trust**.

**Step 4** *(Optional)* Enter a description in the **Description** field and select **Browse**.

**Step 5** Browse to the location where you saved the public certificates in .pem format, and select one of the converted certificates.

**Step 6** Select **Upload File**.

**Step 7** Repeat Step 2 through Step 6, but select **Unity Connection-trust** in the Certificate Name list.

**Step 8** If you have public certificates from more than one certification authority, repeat Step 2 through Step 7 for the remaining certificates.

# Uploading Certificates for Office 365 and Cisco Unity Connection

At the time of creating unified messaging services, if you select "Validate Certificates for Exchange Servers" for Office 365, you must perform the following steps to upload Office 365 root certificate to the tomcat-trust of Cisco Unity Connection.

**Step 1** Select the Office 365 EWS endpoint URL https://outlook.office365.com/EWS/Exchange.ASMX and download the Office 365 root certificate.

**Step 2** In Cisco Unified Operating System Administration, expand Security and select Certificate Management.

**Step 3** On the Certificate Management page, select Upload Certificate.

**Step 4** In the Certificate Name list, select tomcat-trust.

**Step 5** *(Optional)* Enter a description in the **Description** field and select Browse

**Step 6** Browse to the location where you saved the Office 365 root certificate, and select the certificate.

**Step 7** Select Upload File.

**Caution** If Office 365 EWS endpoint URL communicates with Cisco Unity Connection through a different root certificate, the same must be uploaded to the tomcat-trust of Cisco Unity Connection.

# Settings Configured on Unity Connection Users

**Step 1** In Cisco Unity Connection Administration, expand **Class of Service** and select **Class of Service**. On the Search Class of Service page, select the class of service assigned to users in which you want to configure unified messaging. (For information on each field, see **Help> This Page**).

**Step 2** On the Edit Class of Service page, in the **Licensed Features** section, check the **Allow Users to Access Voicemail Using an IMAP Client and/ or Single Inbox** check box.

**Step 3** You must configure message aging or message quotas. For more information, see the "Message Storage" chapter of the *System Administration Guide for Cisco Unity Connection, Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html

**Note** If you want to permanently delete the messages from Web Inbox, check the **Delete Messages Without Saving to Deleted Items Folder** check box in the **Message Options** section.

**Step 4** (*for Text-to-Speech feature only*): In the **Licensed Features** section, check the **Allow Access to Advanced Features** and the **Allow Access to Exchange Email by Using Text to Speech (TTS)** check boxes.

**Step 5** Select **Save**.

# Unified Messaging Account for Users

## Unified Messaging Accounts and User Accounts Related for Unity Connection

Unified messaging accounts connect Unity Connection users to unified messaging services. Unified messaging accounts are separate objects from user accounts:

- When you create a user account, Unity Connection does not automatically create a unified messaging account for that user.
- You can create more than one unified messaging account for a user, but a user's unified messaging accounts cannot have overlapping features. For example, you cannot create two unified messaging accounts for the same user that both enable single inbox.
- Creating multiple unified messaging accounts for a user is one way to control access to unified messaging features. For example, if you want all users to have single inbox but only a few users to have text-to-speech access to Exchange email, you can create two unified messaging services. One activates single inbox and the other activates TTS. You then create unified messaging accounts for all users to give them access to single inbox, and you create a second unified messaging account for the users who you want to have TTS.
- When you add a unified messaging account, the associated user account is updated with a reference to the unified messaging account. The user account does not contain the information on the unified messaging account.
- When you delete a user account, all unified messaging accounts for that user are also deleted. However, when you delete a unified messaging account, the corresponding user account is not deleted. The user account is updated only to remove the reference to the unified messaging account.

## Creating Unified Messaging Accounts for Users

You can create a large number of unified messaging accounts using Bulk Administration Tool. For information on creating, updating, or deleting unified messaging accounts using BAT tool, see the "Bulk Administration Tool" section of the "Tools" chapter of the *System Administration Guide for Cisco Unity Connection, Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html.

For information on synchronization behavior if you later disable single inbox in a unified messaging account, see the "Moving and Restoring Exchange Mailboxes" chapter.

**Step 1** In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select **Add New** to create a new user or select an applicable user for which you want to create a unified messaging account.

**Step 2** Configure unified messaging account (For information on each field, see **Help> This Page**):

a) In the **Edit** menu, select **Unified Messaging Accounts**.
b) On the Unified Messaging Accounts page, select **Add New**.
c) On the New Unified Messaging Accounts page, enter the values of the required fields and select **Save**.

**Step 3** To check the configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for the mail server, Active Directory, Unity Connection, and the Unity Connection user.

# Test Unified Messaging Configuration

## View the Summary of Unified Messaging Configuration

You can view a summary of the configuration for all of the unified messaging accounts on a Unity Connection server, including:

- Current status of Unity Connection configuration settings for each unified messaging account that indicates whether consistency problems with Unity Connection settings prevent unified messaging from functioning correctly. When you select the status icon for a unified messaging account, the Unified Messaging Account page appears, and the status area of the page lists both problems and possible problems, if any.
- You can also test whether a unified messaging account has connectivity with other servers using the **Test Connectivity** button on the Unified Messaging Account page.
- The alias of the user associated with the account. When you select the alias for a unified messaging account, the Edit Unified Messaging Account page appears, and the status area of the page lists problems and possible problems, if any.
- The display name of the user associated with the unified messaging account.
- The name of the unified messaging service that is associated with the unified messaging account. When you select the service name, the Unified Messaging Services page appears with the settings for the service.
- The current unified messaging settings for each unified messaging account.

### Viewing a Summary of Configuration of Unified Messaging Accounts for Unity Connection

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

**Step 2** To sort by the values in a column in ascending order, select the heading for the column. To sort in descending order, select the heading again.

**Step 3** View the following settings:

- To display the Unified Messaging Accounts page for an account, select the icon or the value of the **Alias** column in the applicable row.
- To display the Unified Messaging Services page for an account, select the value of the **UM Services** column in the applicable row.

## Testing System Configuration and Unified Messaging with Exchange 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.

Do the following to check the system configuration and unified messaging configuration:

**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 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 Calendars for Unity Connection

If you configured Unity Connection to calendars, do the following procedure to test the access to calendars.

**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. Select **Send**.

**Step 5** Sign in to the Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

**Step 6** 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 follow the prompts to list meetings. Unity Connection reads the information about the meeting.

## Resolving SMTP Domain Name Configuration Issues

When a single inbox user receives a voicemail, it is synchronized from Unity Connection to a mail server. The email address of sender/recipient has Unity Connection domain name, for example, userid@CUC-hostname. Due to this, email clients like Microsoft Outlook or IBM Lotus Notes adds the Unity Connection address as “recent contacts” in the address book. When a user replies to an email or adds recipient while composing an email, the user can enter/select the Unity Connection address, which may lead to NDR. You must follow the steps further if you want the email address of sender/recipient to be displayed as the corporate email address, for example, userid@corp-hostname, when the voicemail is synchronized for single inbox users from Unity Connection to the mail server.

Do the following procedure to resolve SMTP domain name configuration issues:

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

**Step 2** On the Smart Host page, enter the values of the required fields and select **Save** (For information on each field, see **Help> This Page**).

**Note** Microsoft Exchange server can be used as a smart host.

**Step 3** Configure corporate email address of a user:

a) In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users page, select an applicable user.
b) On the Edit User Basics page, enter value in the **Corporate Email Address** field and select **Save**.

**Step 4** In Cisco Unity Connection Administration, expand **System Settings** and select **General Configuration**.

**Step 5** On the General Configuration page, in the **When a recipient cannot be found** list, select **Relay message to smart host** so that if the Recipient is not found, the message is sent to the smart host and select **Save**.

**Step 6** Configure message action for a user:

a) In Cisco Unity Connection Administration, expand **Users** and select **Users**. On the Search Users Basics page, select an applicable user.
b) On the Edit User Basics page, in the **Edit** menu, select **Message Actions**. On the Edit Message Actions page, select the **Accept the Message** option from the **Voicemail** drop- down list.

**Note** Make sure to select the **Relay the Message** option from the Email, Fax, and receipt drop -down lists.

**Step 7** Setup a recipient policy on the mail server so that the Unity Connection alias resolves to the **Corporate Email Address ID:**

- For Exchange 2019 or Exchange 2016, see the following link:

  http://technet.microsoft.com/en-us/library/bb232171.aspx