Configuring Unified Messaging

Cisco Unity Connection can be integrated with Microsoft Exchange 2016, 2013, 2010, Office 365, and Cisco Unified MeetingPlace to deploy the unified messaging feature.

- Configuring Unified Messaging, on page 1

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 2010 client access server, Unity Connection can access Exchange 2010 mailboxes in the Exchange organization, but cannot access Exchange 2013 mailboxes or Exchange 2016 mailboxes.

- If you select a specific Exchange 2013 client access server, Unity Connection can access all Exchange 2013, Exchange 2010 mailboxes in the Exchange organization, but cannot access Exchange 2016 mailboxes.

- If you allow Unity Connection to search for Exchange servers, you need to give permissions to the Exchange servers. See the following sections to grant permissions to the applicable Exchange server:
  - Granting Permissions for Exchange 2013 or Exchange 2016
  - Granting Permissions for Exchange 2010
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: Adding Unified Messaging Services Based on Versions of Exchange explains when you need to add more than one unified messaging service.

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

<table>
<thead>
<tr>
<th>Exchange Versions with Mailboxes That You Want Unity Connection to be Able to Access</th>
<th>Create the Following Unified Messaging Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2010</td>
<td>Exchange 2013</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>- One for Office 365 server that you want Unity Connection to be able to access.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>- One for Exchange 2016.</td>
<td></td>
</tr>
<tr>
<td>- One for Office 365 server that you want Unity Connection to be able to access.</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>- One for Exchange 2016. This service can also access Exchange 2013 mailboxes.</td>
<td></td>
</tr>
<tr>
<td>- One for Office 365 server that you want Unity Connection to be able to access.</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- One for Exchange 2016. This service can also access Exchange 2013 and Exchange 2010 mailboxes.</td>
<td></td>
</tr>
<tr>
<td>- One for Office 365 server that you want Unity Connection to be able to access.</td>
<td></td>
</tr>
</tbody>
</table>
### Create the Following Unified Messaging Services

<table>
<thead>
<tr>
<th>Exchange 2010</th>
<th>Exchange 2013</th>
<th>Exchange 2016</th>
<th>Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- One for Exchange 2016. This service can also access Exchange 2013, Exchange 2010 mailboxes.
- One for Office 365 server that you want Unity Connection to be able to access.

- One for Exchange 2013. This service can also access Exchange 2010 mailboxes.
- One for Office 365 server that you want Unity Connection to be able to access.

- One for Office 365 server that you want Unity Connection to be able to access.

- One for Exchange 2013. This service can also access Exchange 2010 and 2007 mailboxes.
- One for Office 365 server that you want Unity Connection to be able to access.

- One for Office 365 server that you want Unity Connection to be able to access.
### Create the Following Unified Messaging Services

<table>
<thead>
<tr>
<th>Exchange 2010</th>
<th>Exchange 2013</th>
<th>Exchange 2016</th>
<th>Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **One for Exchange 2013.** This service can also access Exchange 2010 mailboxes.
- **One for Exchange 2013.** This service can also access Exchange 2010 mailboxes.
- **One for Office 365 server that you want Unity Connection to be able to access.**
- **One for Office 365 server that you want Unity Connection to be able to access.**
- **One for Exchange 2013.** This service can also access Exchange 2010 mailboxes.
- **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: Choosing a Specific Exchange Server: When Unity Connection Detect Moving a Mailbox Between Exchange Servers

<table>
<thead>
<tr>
<th>If you select a specific Exchange server</th>
<th>Unity Connection can automatically detect mailbox moves between the following Exchange versions</th>
</tr>
</thead>
</table>

- 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.

---

**Prerequisites for Configuring Unified Messaging**

Following prerequisites should be met before configuring unified messaging with any supported mail servers:


2. Ensure that you have sufficient licenses for the voicemail users:
   1. Navigate to Cisco Unity Connection Administration, expand System Settings and select Licenses.
   2. 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 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 **EmailAddress** field is specified.

---

**Task List for Configuring Unified Messaging**

**Task List for Configuring Unified Messaging with Exchange 2013 or Exchange 2016**

---

**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 2013 or Exchange 2016. 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 2013 or Exchange 2016 server, or you want Unity Connection to communicate with a specific Exchange 2013 or Exchange 2016 server in case the hostname or the IP Address of the specific server is known. Do the following steps:

a) **Granting Permissions for Exchange 2013 or Exchange 2016**

b) **(Optional) Confirming Exchange 2013 or Exchange 2016 Authentication and SSL Settings**

c) **Task List for Configuring Unified Messaging with Exchange 2010**

**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.


**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.
Task List for Configuring Unified Messaging with Exchange 2010

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 Exchange 2010. 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 2010 server, or you want Unity Connection to communicate with a specific Exchange 2010 server in case the hostname or the IP Address of the specific server is known. Follow the given steps:
   a)  Granting Permissions for Exchange 2010
   b)  (Optional) Confirming Exchange 2010 Authentication and SSL Settings
   c)  Depending on applicable version:
      • Configuring EWS Limits on Exchange 2010 SP2 RU4 and Later
      • Configuring EWS Limits on Exchange 2010 SP2 RU3 and Earlier Releases

   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 already 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.


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 3b., configure unified messaging services to validate certificates for Exchange servers in Step 8.
• If you 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 in Step 8.

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, in Step 8 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 the Granting 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.

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

Step 4 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) Assigning Application Impersonation Role for Office 365

For more information, see the "Latency" section of the “Single Inbox” chapter in the Design Guide for Cisco Unity Connection, Release 12.x, available at:
Step 6  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.


Step 7  (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 8  Configure one or more unified messaging services on Unity Connection. For more information, see the Granting Permissions section.

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

Step 10  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 11  Test the unified messaging service. For more information, see the Test Unified Messaging Configuration section.

Task for Configuring Unified Messaging

Configuring Unified Messaging in Active Directory

Unity Connection accesses Exchange or Office 365 mailboxes using an Active Directory 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.

For Office 365, Exchange 2016, Exchange 2013, and Exchange 2010, operations are performed through Exchange Web Services (EWS). Uploading messages into Exchange mailboxes:

• 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.
You need to create one or more domain user accounts in the Active Directory forest that includes the Exchange 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.

• Do not add the account to any administrator group.

• Do not disable the account or Unity Connection cannot use it to access Exchange or Office 365 mailboxes.

• Specify a password that satisfies the password-security requirements of your company.

---

**Note**  
The password is encrypted with AES 128-bit encryption and stored in the Unity 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 cluster, Unity Connection automatically uses the same unified messaging services account for both Unity 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 Unity Connection servers. However, this is not a requirement and does not affect functionality or performance.

---

**Granting Permissions**

**Granting Permissions for Exchange 2013 or Exchange 2016**

**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 2013 or Exchange 2016:

```
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 2013 or Exchange 2016, you need to assign the Application Impersonation management role to the unified messaging service account.
Granting Permissions for Exchange 2010

**Step 1**  Sign into 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 2010:

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

where:

- **RoleName** is the name that you want to give the assignment, for example, UnityConnectionUMServicesAcct. 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.

When configuring unified messaging service account for Exchange 2010, you need to assign the Application Impersonation management role to the unified messaging service account.


**Step 3**  *(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 configured Exchange to use HTTPS in Step 3b, configure unified messaging services to validate certificates for Exchange servers.

- If you 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 4**  Configure one or more unified messaging services on Unity Connection. For more information, see the Creating a Unified Messaging Service to Access Mail Server section.

**Step 5**  Update the settings for unified messaging users. For more information, see the Settings Configured on Unity Connection Users section.

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.
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 2013 or Exchange 2016 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 2013 or Exchange 2016 client access servers. You must configure all Exchange 2013 or Exchange 2016 client access servers to use the same type of authentication.

Step 2
Decide whether you want the communication between Unity Connection and Exchange 2013 or Exchange 2016 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on all the Exchange 2013 or Exchange 2016 client access servers.

Step 3
Sign in to a server that has access to the same Exchange 2013 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 2013 or Exchange 2016 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 2013 or Exchange 2016 client access servers that Unity Connection can access.

Step 9  Close IIS Manager.

Confirming Exchange 2010 Authentication and SSL Settings

Step 1  Decide the type of authentication (Basic, Digest, or NTLM) you want Unity Connection to use to sign in to Exchange 2010 client access servers. You must configure the following servers to use the same type of authentication:
   • All Exchange 2010 client access servers.

Step 2  Decide whether you want the communication between Unity Connection and Exchange 2010 client access servers to be SSL encrypted. If so, you must specify the same SSL setting on the following servers:
   • All Exchange 2010 client access servers.

Step 3  Sign in to a server that has access to the same Exchange 2010 client access servers that Unity Connection has. 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 2010 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 Autodiscover and EWS.

Step 6  Under Default Website, select Autodiscover:
   a) In the middle pane, in the IIS section, double-click Authentication.
Confirm that the Status column states **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 the following types of authentication:

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

b) If you 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) If the **Require SSL** check box is checked:
   - When you create a unified messaging service in Unity Connection, you must select HTTPS for the web-based protocol.
   - 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 says **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 in.

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 changed any settings, in the right pane, select **Apply**.

g) If you have installed Exchange 2010 Service Pack 1 or later, skip to **Step 8**.

If you have not installed Exchange 2010 Service Pack 1 or later, edit the Exchange web.config files for EWS and for autodiscovery to match the settings in IIS Manager:

- For EWS, see “**Enable or Disable SSL on Exchange Web Services Virtual Directories**” on the Microsoft Technet website.
Step 8 Repeat Step 5 through Step 6 for the other Exchange 2010 client access servers that Unity Connection can access.

Step 9 Close IIS Manager.

Configuring Paged View Functionality in Unity Connection for Exchange 2013 or Exchange 2016

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.

Configuring EWS Limits for Exchange 2010

Configuring EWS Limits on Exchange 2010 SP2 RU4 and Later

Microsoft has enabled the client throttling policy feature by default. If there is no throttling policy already configured, Microsoft Exchange applies a default policy to all users. The default throttling policy is tailored for end user's load and not for an enterprise application like, Unity Connection using impersonation. If any Unity Connection users who are configured for unified messaging have mailboxes in Exchange 2010, configure the Exchange 2010 EWS limits for the unified messaging users mailbox by creating and applying a new mailbox policy to the unified messaging user mailbox account. If you do not configure EWS limits, messages may not be synchronized, and status changes (for example, from unread to read), changes to the subject line,
and changes to the priority may not be replicated. In addition, attempts to access Exchange calendars and contacts may fail.

Note Prior to Exchange 2010 SP2 RU4, the throttling limit was calculated against the calling account (In Our Case Service Account). Starting with, Exchange 2010 SP2 RU4, this limit has been changed. Now, the charges are counted against the target mailbox instead of the calling account.

Note Make sure to enable the paged view functionality for FindItem calls. For more information on how to enable the paged view functionality, see the Configuring Paged View Functionality in Unity Connection for Exchange 2013 or Exchange 2016 section. If you have the paged view functionality disabled, configure the EWS limits by following the below steps.

**Configuring EWS Limits for Unified Messaging Users**

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

### Step 2
Create a new policy with the following EWS connections where Exchange mailboxes have more than 1000 messages, which includes voicemails and receipts. For Exchange mailboxes with 10000 messages, then the new throttling policy is

```
New-ThrottlingPolicy -Name "<ConnectionUnifiedMessagingServicesPolicy>" -EWSPercentTimeInCAS 300
-EWSPercentTimeInMailboxRPC 200 -EWSFindCountLimit 10000 -EWSPercentTimeinAD 100
```

where *ConnectionUnifiedMessagingServicesPolicy* is the name that you want to assign to the policy. Refer to the Table 3: Recommended Throttle Policy Parameter Values With 10000 Items in User’s Mailbox section to have detailed description on the throttling policy parameters.

Apply the new policy to all the unified messaging user mailbox. For each user mailbox, run the following command:

```
Set-ThrottlingPolicyAssociation -Identity "<ConnectionUnifiedMessagingusermailbox>" -ThrottlingPolicy
"<ConnectionUnifiedMessagingServicesPolicy>"
```

where:

- *ConnectionUnifiedMessagingusermailbox* is the name of the user mailbox.
- *ConnectionUnifiedMessagingServicesPolicy* is the name of the policy that you created in Step 2.

### Step 3
Confirm that the mailbox is using the new policy:

```
Get-ThrottlingPolicyAssociation -Identity "<ConnectionUnifiedMessagingusermailbox>" | findstr "ThrottlingPolicy"
```

### Step 4
On each Exchange 2010 server that has the CAS role, restart the Microsoft Exchange RPC Client Access service.
Table 3: Recommended Throttle Policy Parameter Values With 10000 Items in User’s Mailbox

<table>
<thead>
<tr>
<th>Field</th>
<th>Policy Value To Be Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EWSPercentTimeInCAS</td>
<td>300</td>
<td>Specifies the percentage of a minute that an Exchange Web Services user can spend executing the client access server code (PercentTimeInCAS).</td>
</tr>
<tr>
<td>EWSPercentTimeInMailboxRPC</td>
<td>200</td>
<td>Specifies the percentage of a minute that an Exchange Web Services user can spend executing mailbox remote procedure call (RPC) requests (PercentTimeInMailboxRPC).</td>
</tr>
<tr>
<td>EWSFindCountLimit</td>
<td>10000</td>
<td>Defines the maximum number of items from a FindItem or FindFolder operation that can exist in memory on the Client Access server at one time for one user. Note: If in your deployment mailboxes have more than 10,000 messages, then you can adjust this parameter.</td>
</tr>
<tr>
<td>EWSPercentTimeinAD</td>
<td>100</td>
<td>Specifies the maximum amount of time that can be spent by a Client Access server when accessing Active Directory resources on behalf of a client account, per minute.</td>
</tr>
</tbody>
</table>

Configuring EWS Limits on Exchange 2010 SP2 RU3 and Earlier Releases

If any Unity Connection users who are configured for unified messaging have mailboxes in Exchange 2010, configure the Exchange 2010 EWS limits for the unified messaging service account by creating and applying a new mailbox policy to the unified messaging services account. If you do not configure EWS limits, messages may not be synchronized, and status changes (for example, from unread to read), changes to the subject line, and changes to the priority may not be replicated. In addition, attempts to access Exchange calendars and contacts may fail.

Note: Prior to Exchange 2010 Service Pack 1, EWS limits were off by default. If you have not yet installed Service Pack 1, which turns limits on by default, we still recommend that you do the following procedure. Otherwise, when you install Service Pack 1, Unity Connection functionality is affected.

Removing EWS Limits for Unified Messaging Users (Exchange 2010 SP2 RU3 and Earlier Releases)

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

Step 2  Create a new policy with unlimited EWS connections:
New-ThrottlingPolicy -Name "<ConnectionUnifiedMessagingServicesPolicy>" -EWSMaxConcurrency $null
-EWSMaxSubscriptions $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null
-EWSFindCountLimit $null -EWSPercentTimeinAD $null

where ConnectionUnifiedMessagingServicesPolicy is the name that you want to assign to the policy.

Step 3
Apply the new policy to the unified messaging services account and the user mailbox:

Set-ThrottlingPolicyAssociation -Identity "<ConnectionUnifiedMessagingServicesAccount>" -ThrottlingPolicy "<ConnectionUnifiedMessagingServicesPolicy>"

where:
• ConnectionUnifiedMessagingServicesAccount is the name of the account that you created in the Configuring Unified Messaging in Active Directory.
• ConnectionUnifiedMessagingServicesPolicy is the name of the policy that you created in Step 2.

Note The Set-ThrottlingPolicyAssociation command is not supported with Exchange 2010 version 14.00.0639.021. The users with Exchange 2010 version 14.00.0639.021 are not allowed to modify an existing throttling policy settings, hence the default policy gets applied here.

Step 4
Confirm that the mailbox is using the new policy:

Get-ThrottlingPolicyAssociation -Identity "<ConnectionUnifiedMessagingServicesAccount>" | findstr "ThrottlingPolicy"

Step 5
If you have created more than one unified messaging services account, repeat Step 3 and Step 4 for the remaining accounts.

Step 6
On each Exchange 2010 server that has the CAS role, restart the Microsoft Exchange RPC Client Access service.

Table 4: Throttling Policy Parameter Descriptions and Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Policy Value to Be Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EWSMaxConcurrency</td>
<td>Null</td>
<td>Specifies how many concurrent connections an Exchange Web Services user can have against an Exchange server at one time.</td>
</tr>
<tr>
<td>EWSMaxSubscriptions</td>
<td>Null</td>
<td>Specifies the maximum number of active push and pull subscriptions that a user can have on a specific Client Access server at the same time.</td>
</tr>
<tr>
<td>EWSPercentTimeInCAS</td>
<td>Null</td>
<td>Specifies the percentage of a minute that an Exchange Web Services user can spend executing the client access server cod (PercentTimeInCAS).</td>
</tr>
<tr>
<td>EWSPercentTimeInMailboxRPC</td>
<td>Null</td>
<td>Specifies the percentage of a minute that an Exchange Web Services user can spend executing mailbox remote procedure call (RPC) requests (PercentTimeInMailboxRPC)</td>
</tr>
<tr>
<td>EWSFindCountLimit</td>
<td>Null</td>
<td>Defines the maximum number of items from a FindItem or FindFolder operation that can exist in memory on the Client Access server at one time for one user.</td>
</tr>
</tbody>
</table>
### Configuring Unified Messaging

#### Accessing Office 365 Using Remote Exchange Management Power Shell

<table>
<thead>
<tr>
<th>Field</th>
<th>Policy Value to Be Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EWSPercentTimeinAD</td>
<td>Null</td>
<td>Specifies the maximum amount of time that can be spent by a Client Access server when accessing Active Directory resources on behalf of a client account, per minute.</td>
</tr>
</tbody>
</table>

#### 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
```

**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.

### 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 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/security/b_12xcucsecx.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:

   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:

- 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**  

**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**  

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

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 12.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.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...
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 12.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.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 Account 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.
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**.
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.


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 2016, Exchange 2013 or Exchange 2010, see the following link:
Resolving SMTP Domain Name Configuration Issues