



# Setting Up a Cisco Unified Communications Manager 8.x, 9.x, and 10.x SIP Trunk Integration with Cisco Unity Connection

For detailed instructions for setting up a Cisco Unified Communications Manager 10.x SIP trunk integration with Cisco Unity Connection, see the following sections in this chapter:

- [Integration Tasks, page 6-1](#)
- [Requirements, page 6-2](#)
- [Centralized Voice Messaging, page 6-3](#)
- [Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection, page 6-3](#)
- [Creating a New Integration with Cisco Unified Communications Manager, page 6-19](#)

This document applies only when Cisco Unity Connection is installed on a separate server from Cisco Unified CM. This document does not apply to the configuration in which Cisco Unity Connection is installed as Cisco Business Edition—on the same server with Cisco Unified CM.



**Note**

If you are configuring MWI relay across trunks in a distributed phone system, you must see the Cisco Unified CM documentation for requirements and instructions. Configuring MWI relay across trunks does not involve Cisco Unity Connection settings.

Cisco Unified CM Music on Hold (MOH) feature is not available during supervised transfers for the Cisco Unified CM SIP trunk integration.

## Integration Tasks

Before doing the following tasks to integrate Cisco Unity Connection with Cisco Unified CM through a SIP trunk, confirm that the Cisco Unity Connection server is ready for the integration by completing the applicable tasks in the *Installation Guide for Cisco Unity Connection*.

1. Review the system and equipment requirements to confirm that all phone system and Cisco Unity Connection server requirements have been met. See the [“Requirements” section on page 6-2](#).
2. Plan how the voice messaging ports will be used by Cisco Unity Connection. See [Chapter 2, “Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection.”](#)

3. If Cisco Unity Connection will use IPv6 or dual-mode IPv4 and IPv6 to communicate with Cisco Unified CM, do the following subtasks:
  - a. Enable IPv6 on the Cisco Unity Connection server. See the “Ethernet IPv6 Configuration Settings” section in the “Settings” chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x* at [http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html).
  - b. In Cisco Unity Connection Administration, on the System Settings > General Configuration page, select an option for IP Addressing Mode to control where Cisco Unity Connection listens for incoming traffic. You can select IPv4, IPv6, or IPv4 and IPv6. The setting defaults to IPv4.
4. Program Cisco Unified CM. See the “Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection” section on page 6-3.
5. Create the integration. See the “Creating a New Integration with Cisco Unified Communications Manager” section on page 6-19.




---

**Note** An additional Cisco Unified CM cluster can be added by adding a new phone system, port group, and ports. Each Cisco Unified CM cluster is a separate phone system integration.

---

6. Test the integration. See Chapter 7, “Testing the Integration.”
7. If this integration is a second or subsequent integration, add the applicable new user templates for the new phone system. See Chapter 8, “Adding New User Templates for Multiple Integrations.”

## Requirements

The Cisco Unified CM SIP integration supports configurations of the following components:

### Phone System

- Cisco Unified CM 10.x

For details on compatible versions of Cisco Unified CM, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at [http://www.cisco.com/en/US/products/ps6509/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html).

- For the Cisco Unified CM extensions, one of the following configurations:
  - (Best practice) Only SIP phones that support DTMF relay as described in RFC-2833.
  - Both SCCP phones and SIP phones.

Note that older SCCP phone models may require a Media Termination Point (MTP) to function correctly.
- A LAN connection in each location where you will plug the applicable phone into the network.
- For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Cisco Unified CM cluster without having to dial a trunk access code or prefix.

### Cisco Unity Connection Server

- The applicable version of Cisco Unity Connection. For details on compatible versions of Cisco Unity Connection, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at [http://www.cisco.com/en/US/products/ps6509/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html).

- Cisco Unity Connection installed and ready for the integration, as described in the *Installation Guide for Cisco Unity Connection* at [http://www.cisco.com/en/US/products/ps6509/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html).
- A license that enables the applicable number of voice messaging ports.

## Centralized Voice Messaging

Cisco Unity Connection supports centralized voice messaging through the phone system, which supports various inter-phone system networking protocols including proprietary protocols such as Avaya DCS, Nortel MCDN, or Siemens CorNet, and standards-based protocols such as QSIG or DPNSS. Note that centralized voice messaging is a function of the phone system and its inter-phone system networking, not voicemail. Unity Connection will support centralized voice messaging as long as the phone system and its inter-phone system networking are properly configured. For details, see the “Centralized Voice Messaging” section in the “Integrating Cisco Unity Connection with the Phone System” chapter of the *Design Guide for Cisco Unity Connection Release 10.x* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/10x/design/guide/10xcucdgx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html).

## Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection

After the Cisco Unified CM software is installed, do the procedures in the applicable section:

- **Cisco Unity Connection without a Unity Connection cluster**—Do the procedures in the “For Cisco Unity Connection Without a Unity Connection Cluster” section on page 6-3.
- **Cisco Unity Connection with a Unity Connection cluster configured**—Do the procedures in the “For Cisco Unity Connection with a Unity Connection Cluster Configured” section on page 6-10.

### For Cisco Unity Connection Without a Unity Connection Cluster

Revised April 17, 2014

Do the following procedures in the order given.



#### Note

There must be a calling search space that is used by all user phones (directory numbers). Otherwise, the integration will not function correctly. For instructions on setting up a calling search space and assigning user phones to it, see the Cisco Unified CM Help.

#### To Create the SIP Trunk Security Profile

- Step 1** In Cisco Unified CM Administration, on the System menu, select **Security > SIP Trunk Security Profile**.
- Step 2** On the Find and List SIP Trunk Security Profiles page, select **Add New**.
- Step 3** On the SIP Trunk Security Profile Configuration page, under SIP Trunk Security Profile Information, enter the following settings.

**Table 6-1 Settings for the SIP Trunk Security Profile Configuration Page**

Field	Setting
Name	Enter <b>Unity Connection SIP Trunk Security Profile</b> or another name.
Description	Enter <b>SIP trunk security profile for Cisco Unity Connection</b> or another description.
Device Security Mode	<p>If you will not enable Cisco Unified CM authentication and encryption, accept the default of <b>Non Secure</b>.</p> <p>If you will enable Cisco Unified CM authentication or encryption, select <b>Authenticated</b> or <b>Encrypted</b>. Note the following requirements for the Cisco Unified CM server:</p> <ul style="list-style-type: none"> <li>• A TFTP server must be configured.</li> <li>• The Cisco Unified CM server must be configured for security by using the Cisco CTL client. For details, see the “Configuring the Cisco CTL Client” section of the “Configuring the Cisco CTL Client” chapter in the <i>Cisco Unified Communications Manager Security Guide</i> at <a href="http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_5_1/secugd/secuauth.html">http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_5_1/secugd/secuauth.html</a>.</li> <li>• The Device Security Mode setting on the Cisco Unified CM server must match the Security Mode setting on the Cisco Unity Connection server (Authenticated or Encrypted).</li> </ul>
X.509 Subject Name	<p>If you will not enable Cisco Unified CM authentication and encryption, leave this field blank.</p> <p>If you will enable Cisco Unified CM authentication and encryption, enter <b>Connection</b> or another name. This name must match the Subject Name field for the SIP certificate on the Cisco Unity Connection server.</p>
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Check this check box.

**Step 4** Select **Save**.

---

### To Create the SIP Profile

**Step 1** On the Device menu, select **Device Settings > SIP Profile**.

**Step 2** On the Find and List SIP Profiles page, select **Find**.

**Step 3** To the right of the SIP profile that you want to copy, select **Copy**.

**Step 4** On the SIP Profile Configuration page, under SIP Profile Information, enter the following settings.

**Table 6-2 Settings for the SIP Profile Configuration Page**

Field	Setting
Name	Enter <b>Unity Connection SIP Profile</b> or another name.
Description	Enter <b>SIP profile for Cisco Unity Connection</b> or another description.

**Step 5** If Cisco Unity Connection will use IPv6 or dual-stack IPv4 and IPv6 to communicate with Cisco Unified CM, check the Enable ANAT check box. This step is required to ensure proper handling of callers in an IPv6 or dual-stack environment.

**Step 6** Select **Save**.

### To Create the SIP Trunk

**Step 1** On the Device menu, select **Trunk**.

**Step 2** On the Find and List Trunks page, select **Add New**.

**Step 3** On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.

**Step 4** In the Device Protocol field, select **SIP** and select **Next**.

**Step 5** Under Device Information, enter the following settings.

**Table 6-3 Settings for Device Information on the Trunk Configuration Page**

Field	Setting
Device Name	Enter <b>Unity_Connection_SIP_Trunk</b> or another name.
Description	Enter <b>SIP trunk for Cisco Unity Connection</b> or another description.
SRTP Allowed	If you will enable Cisco Unified CM authentication and encryption, check this check box.

**Step 6** If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to [Step 7](#).

**Table 6-4 Settings for Inbound Calls on the Trunk Configuration Page**

Field	Setting
Calling Search Space	Select the name of the calling search space that contains the user phones.
Redirecting Diversion Header Delivery - Inbound	Check this check box.

**Step 7** If user phones are contained in a calling search space, under Outbound Calls, enter the following settings.

**Table 6-5 Settings Outbound Calls on Trunk Configuration Page**

Field	Setting
Redirecting Diversion Header Delivery - Outbound	Check this check box.
Deliver DN only in connected party	In outgoing SIP messages, Unity Connection inserts the calling party's directory number in the SIP contact header information. This is the default setting.
Deliver URI only in connected party	In outgoing SIP messages, Unity Connection inserts the sending party's directory URI in the SIP contact header. If a directory URI is not available, Unity Connection inserts the directory number instead.
Deliver URI and DN in connected party	In outgoing SIP messages, Unity Connection inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unity Connection includes the directory number only.

**Step 8** Under SIP Information, enter the following settings.

**Table 6-6 Settings for SIP Information on the Trunk Configuration Page**

Field	Setting
Destination Address	Enter the IP address of the Cisco Unity Connection SIP port to which Cisco Unified CM will connect.
Destination Address IPv6	Enter the IPv6 address of the Cisco Unity Connection SIP port to which Cisco Unified CM will connect. <b>Note</b> IPv6 is supported for SIP integrations between Unity Connection and Cisco Unified CM .
Destination Port	We recommend that you accept the default of <b>5060</b> .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the <a href="#">“To Create the SIP Trunk Security Profile” procedure on page 6-3</a> . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the <a href="#">“To Create the SIP Profile” procedure on page 6-4</a> . For example, select “Cisco Unity Connection SIP Profile.”

**Step 9** Adjust any other settings that are needed for your site.

**Step 10** Select **Save**.

---

### To Create a Route Pattern

---

**Step 1** On the Call Routing menu, select **Route/Hunt > Route Pattern**.

**Step 2** On the Find and List Route Patterns page, select **Add New**.

**Step 3** On the Route Pattern Configuration page, enter the following settings.

**Table 6-7 Settings for the Route Pattern Configuration Page**

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the SIP trunk that you created in the <a href="#">“To Create the SIP Trunk” procedure on page 6-5</a> . For example, select “Unity_Connection_SIP_Trunk.”

**Step 4** Select **Save**.

---

#### To Create the Voice Mail Pilot

**Step 1** On the Advanced Features menu, select **Voice Mail > Voice Mail Pilot**.

**Step 2** On the Find and List Voice Mail Pilots page, select **Add New**.

**Step 3** On the Voice Mail Pilot Configuration page, enter the following voice mail pilot number settings.

**Table 6-8 Settings for the Voice Mail Pilot Configuration Page**

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the <a href="#">“To Create a Route Pattern” procedure on page 6-6</a> .
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter <b>Unity Connection Pilot</b> or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

**Step 4** Select **Save**.

---

#### To Set Up the Voice Mail Profile

**Step 1** On the Advanced Features menu, select **Voice Mail > Voice Mail Profile**.

**Step 2** On the Find and List Voice Mail Profiles page, select **Add New**.

**Step 3** On the Voice Mail Profile Configuration page, enter the following voice mail profile settings.

**Table 6-9 Settings for the Voice Mail Profile Configuration Page**

Field	Setting
Voice Mail Profile Name	Enter <b>Unity Connection Profile</b> or another name to identify the voice mail profile.
Description	Enter <b>Profile for Cisco Unity Connection</b> or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the <a href="#">“To Create the Voice Mail Pilot” procedure on page 6-7.</a>
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank.  When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default.  When this check box is checked, this voice mail profile replaces the current default voice mail profile.

**Step 4** Select **Save**.

---

#### To Set Up the Voice Mail Server Service Parameters

---

- Step 1** In Cisco Unified CM Administration, select **System > Service Parameters**.
- Step 2** On the Service Parameters Configuration page, in the Server field, select the name of the Cisco Unified CM server.
- Step 3** In the Service list, select **Cisco CallManager**. The list of parameters appears.
- Step 4** Under Clusterwide Parameters (Feature - General), locate the Multiple Tenant MWI Modes parameter.
- Step 5** If you use multiple tenant MWI notification, select **True**.  
  
When this parameter is set to True, Cisco Unified CM uses any configured translation patterns to convert voicemail extensions into directory numbers when turning on or off an MWI.
- Step 6** If you changed any settings, select **Save**. Then shut down and restart the Cisco Unified CM server.
- 

Do the following two procedures only if you want to set up SIP Digest authentication.

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager” section on page 6-19.](#)

#### (Optional) To Set Up SIP Digest Authentication

---

- Step 1** On the System menu, select **Security > SIP Trunk Security Profile**.



- Step 2** On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile” procedure on page 6-3](#).
- Step 3** On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.
- Step 4** Select **Save**.

---

#### (Optional) To Create the Application User

---

- Step 1** On the User Management menu, select **Application User**.
- Step 2** On the Find and List Application Users page, select **Add New**.
- Step 3** On the Application User Configuration page, enter the following settings.

**Table 6-10 Settings for the Application User Configuration Page**

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, :, \, , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.
Presence Group	Used with the Presence feature, the application user (for example, IPMASysUser) serves as the watcher because it requests status about the presence entity.  If you want the application user to receive the status of the presence entity, make sure that the Application User Presence group is allowed to view the status of the Presence group that is applied to the directory number, as indicated in the Presence Group Configuration window.
Accept Presence Subscription	Leave this check box unchecked.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Leave this check box unchecked.

**Table 6-10** Settings for the Application User Configuration Page (continued)

Field	Setting
Available Devices	<p>This list box displays the devices that are available for association with this application user.</p> <p>To associate a device with this application user, select the device and select the Down arrow below this list box.</p> <p>If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices:</p> <ul style="list-style-type: none"> <li>• <b>Find More Phones</b>—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search.</li> <li>• <b>Find More Route Points</b>—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.</li> </ul>
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.
Groups	The list box displays the groups to which the application user belongs.
Roles	The list box displays the roles that are assigned to the application user.

**Step 4** Select **Save**.

## For Cisco Unity Connection with a Unity Connection Cluster Configured

Do the following procedures in the order given.



**Note**

There must be a calling search space that is used by all user phones (directory numbers). Otherwise, the integration will not function correctly. For instructions on setting up a calling search space and assigning user phones to it, see the Cisco Unified CM Help.

### To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster)

- Step 1** In Cisco Unified CM Administration, on the System menu, select **Security > SIP Trunk Security Profile**.
- Step 2** On the Find and List SIP Trunk Security Profiles page, select **Add New**.
- Step 3** On the SIP Trunk Security Profile Configuration page, under SIP Trunk Security Profile Information, enter the following settings.

**Table 6-11 Settings for the SIP Trunk Security Profile Configuration Page**

Field	Setting
Name	Enter <b>Unity Connection SIP Trunk Security Profile</b> or another name.
Description	Enter <b>SIP trunk security profile for Cisco Unity Connection</b> or another description.
Device Security Mode	<p>If you will not enable Cisco Unified CM authentication and encryption, accept the default of <b>Non Secure</b>.</p> <p>If you will enable Cisco Unified CM authentication or encryption, select <b>Authenticated</b> or <b>Encrypted</b>. Note the following requirements for the Cisco Unified CM server:</p> <ul style="list-style-type: none"> <li>• A TFTP server must be configured.</li> <li>• The Cisco Unified CM server must be configured for security by using the Cisco CTL client. For details, see the “Configuring the Cisco CTL Client” section of the “Configuring the Cisco CTL Client” chapter in the <i>Cisco Unified Communications Manager Security Guide</i> at <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html</a>.</li> <li>• The Device Security Mode setting on the Cisco Unified CM server must match the Security Mode setting on the Cisco Unity Connection server (Authenticated or Encrypted).</li> </ul>
X.509 Subject Name	<p>If you will not enable Cisco Unified CM authentication and encryption, leave this field blank.</p> <p>If you will enable Cisco Unified CM authentication and encryption, enter <b>Connection</b> or another name. This name must match the Subject Name field for the SIP certificate on the Cisco Unity Connection server.</p>
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Check this check box.

**Step 4** Select **Save**.

---

#### To Create the SIP Profile (for a Cisco Unity Connection Cluster)

---

**Step 1** On the Device menu, select **Device Settings > SIP Profile**.

**Step 2** On the Find and List SIP Profiles page, select **Find**.

**Step 3** To the right of the SIP profile that you want to copy, select **Copy**.

**Step 4** On the SIP Profile Configuration page, under SIP Profile Information, enter the following settings.

**Table 6-12 Settings for the SIP Profile Configuration Page**

Field	Setting
Name	Enter <b>Unity Connection SIP Profile</b> or another name.
Description	Enter <b>SIP profile for Cisco Unity Connection</b> or another description.

**Step 5** If Cisco Unity Connection will use IPv6 or dual-stack IPv4 and IPv6 to communicate with Cisco Unified CM, check the Enable ANAT check box. This step is required to ensure proper handling of callers in an IPv6 or dual-stack environment.

**Step 6** Under Parameters Used in Phone, in the Retry INVITE field, enter a value that is 5 or less.

**Step 7** Select **Save**.

---

#### To Create the SIP Trunk (for a Cisco Unity Connection Cluster)

**Step 1** On the Device menu, select **Trunk**.

**Step 2** On the Find and List Trunks page, select **Add New**.

**Step 3** On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.

**Step 4** In the Device Protocol field, select **SIP** and select **Next**.

**Step 5** Under Device Information, enter the following settings.

**Table 6-13 Settings for Device Information on the Trunk Configuration Page**

Field	Setting
Device Name	Enter <b>Unity_Connection_SIP_Trunk_1</b> or another name.
Description	Enter <b>SIP trunk 1 for Cisco Unity Connection</b> or another description.
SRTP Allowed	If you will enable Cisco Unified CM authentication and encryption, check this check box.

**Step 6** If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to [Step 7](#).

**Table 6-14 Settings for Inbound Calls on the Trunk Configuration Page**

Field	Setting
Calling Search Space	Select the name of the calling search space that contains the user phones.
Redirecting Diversion Header Delivery - Inbound	Check this check box.

**Step 7** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.

**Step 8** Under SIP Information, enter the following settings.

**Table 6-15 Settings for SIP Information on the Trunk Configuration Page**

Field	Setting
Destination Address	Enter the IP address of the publisher Cisco Unity Connection server.
Destination Address IPv6	Enter the IPv6 address of the publisher Cisco Unity Connection server. <b>Note</b> IPv6 is supported for SIP integrations between Unity Connection and Cisco Unified CM .
Destination Port	We recommend that you accept the default of <b>5060</b> .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the <a href="#">“To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster)”</a> procedure on page 6-10. For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the <a href="#">“To Create the SIP Profile (for a Cisco Unity Connection Cluster)”</a> procedure on page 6-11. For example, select “Cisco Unity Connection SIP Profile.”

- Step 9** Adjust any other settings that are needed for your site.
- Step 10** Select **Save**.
- Step 11** Select **Add New**.
- Step 12** On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.
- Step 13** In the Device Protocol field, select **SIP** and select **Next**.
- Step 14** Under Device Information, enter the following settings.

**Table 6-16 Settings for Device Information on the Trunk Configuration Page**

Field	Setting
Device Name	Enter <b>Unity_Connection_SIP_Trunk_2</b> or another name.
Description	Enter <b>SIP trunk 2 for Cisco Unity Connection</b> or another description.
SRTP Allowed	If you will enable Cisco Unified CM authentication and encryption, check this check box.

- Step 15** If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to [Step 16](#).

**Table 6-17 Settings for Inbound Calls on the Trunk Configuration Page**

Field	Setting
Calling Search Space	Select the name of the calling search space that contains the user phones.
Redirecting Diversion Header Delivery - Inbound	Check this check box.

**Step 16** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.

**Step 17** Under SIP Information, enter the following settings.

**Table 6-18 Settings for SIP Information on the Trunk Configuration Page**

Field	Setting
Destination Address	Enter the IP address of the subscriber Cisco Unity Connection server.
Destination Address IPv6	Enter the IPv6 address of the subscriber Cisco Unity Connection server. <b>Note</b> IPv6 is supported for SIP integrations between Unity Connection and Cisco Unified CM .
Destination Port	We recommend that you accept the default of <b>5060</b> .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the <a href="#">“To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster)” procedure on page 6-10</a> . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the <a href="#">“To Create the SIP Profile (for a Cisco Unity Connection Cluster)” procedure on page 6-11</a> . For example, select “Cisco Unity Connection SIP Profile.”

**Step 18** Adjust any other settings that are needed for your site.

**Step 19** Select **Save**.

---

### To Create a Route Group (for a Cisco Unity Connection Cluster)

---

**Step 1** On the Call Routing menu, select **Route/Hunt > Route Group**.

**Step 2** On the Find and List Route Groups page, select **Add New**.

**Step 3** On the Route Group Configuration page, enter the following settings.

**Table 6-19 Settings for the Route Group Configuration Page**

Field	Setting
Route Group Name	Enter <b>SIP_Trunk_Route_Group</b> or another name.
Distribution Algorithm	Select <b>Top Down</b> .

- Step 4** Confirm that both SIP trunks appear in the Available Devices field. Otherwise, select **Find**.
- Step 5** Select **Add to Route Group**.
- Step 6** Under Current Route Group Members, confirm that the SIP trunk that connects to the subscriber Cisco Unity Connection server appears first in the list.  
 You can select the up or down arrows to change the order of the SIP trunks.
- Step 7** Select **Save**.

**To Create a Route List (for a Cisco Unity Connection Cluster)**

- Step 1** On the Call Routing menu, select **Route/Hunt > Route List**.
- Step 2** On the Find and List Route Lists page, select **Add New**.
- Step 3** On the Route List Configuration page, enter the following settings.

**Table 6-20 Settings for the Route List Configuration Page**

Field	Setting
Name	Enter <b>SIP_Trunk_Route_List</b> or another name.
Description	Enter <b>SIP Trunk Route List</b> or another description.
Cisco Unified Communications Manager Group	Select <b>Default</b> .

- Step 4** Select **Save**.
- Step 5** Confirm that the **Enable This Route List** check box is checked.
- Step 6** Under Route List Member Information, select **Add Route Group**.
- Step 7** On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the [“To Create a Route Group \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 6-14 and select **Save**.
- Step 8** When prompted that the route list settings will be saved, select **OK**.
- Step 9** On the Route List Configuration page, select **Reset**.
- Step 10** When prompted to confirm resetting the route list, select **Reset**.
- Step 11** Select **Close**.

**To Create a Route Pattern (for a Cisco Unity Connection Cluster)**

- 
- Step 1** On the Call Routing menu, select **Route/Hunt > Route Pattern**.
- Step 2** On the Find and List Route Patterns page, select **Add New**.
- Step 3** On the Route Pattern Configuration page, enter the following settings.

**Table 6-21 Settings for the Route Pattern Configuration Page**

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the route list that you created in the <a href="#">“To Create a Route List (for a Cisco Unity Connection Cluster)”</a> procedure on page 6-15. For example, select “SIP_Trunk_Route_List.”

- Step 4** Select **Save**.
- 

**To Create the Voice Mail Pilot (for a Cisco Unity Connection Cluster)**

- 
- Step 1** On the Advanced Features menu, select **Voice Mail > Voice Mail Pilot**.
- Step 2** On the Find and List Voice Mail Pilots page, select **Add New**.
- Step 3** On the Voice Mail Pilot Configuration page, enter the following voice mail pilot number settings.

**Table 6-22 Settings for the Voice Mail Pilot Configuration Page**

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the <a href="#">“To Create a Route Pattern (for a Cisco Unity Connection Cluster)”</a> procedure on page 6-16.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter <b>Unity Connection Pilot</b> or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

- Step 4** Select **Save**.
- 

**To Set Up the Voice Mail Profile (for a Cisco Unity Connection Cluster)**

- 
- Step 1** On the Advanced Features menu, select **Voice Mail > Voice Mail Profile**.
- Step 2** On the Find and List Voice Mail Profiles page, select **Add New**.



**Step 3** On the Voice Mail Profile Configuration page, enter the following voice mail profile settings.

**Table 6-23 Settings for the Voice Mail Profile Configuration Page**

Field	Setting
Voice Mail Profile Name	Enter <b>Unity Connection Profile</b> or another name to identify the voice mail profile.
Description	Enter <b>Profile for Cisco Unity Connection</b> or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the <a href="#">“To Create the Voice Mail Pilot (for a Cisco Unity Connection Cluster)”</a> procedure on page 6-16.
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank.  When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default.  When this check box is checked, this voice mail profile replaces the current default voice mail profile.

**Step 4** Select **Save**.

Do the following two procedures only if you want to set up SIP Digest authentication.

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 6-19.

**(Optional) To Set Up SIP Digest Authentication (for a Cisco Unity Connection Cluster)**

**Step 1** On the System menu, select **Security > SIP Trunk Security Profile**.

**Step 2** On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 6-10.

**Step 3** On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.

**Step 4** Select **Save**.

**(Optional) To Create the Application User (for a Cisco Unity Connection Cluster)**

**Step 1** On the User Management menu, select **Application User**.

**Step 2** On the Find and List Application Users page, select **Add New**.

**Step 3** On the Application User Configuration page, enter the following settings.

**Table 6-24 Settings for the Application User Configuration Page**

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.
Presence Group	Used with the Presence feature, the application user (for example, IPMASysUser) serves as the watcher because it requests status about the presence entity.  If you want the application user to receive the status of the presence entity, make sure that the Application User Presence group is allowed to view the status of the Presence group that is applied to the directory number, as indicated in the Presence Group Configuration window.
Accept Presence Subscription	Leave this check box unchecked.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Leave this check box unchecked.
Available Devices	This list box displays the devices that are available for association with this application user.  To associate a device with this application user, select the device and select the Down arrow below this list box.  If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices: <ul style="list-style-type: none"> <li>• <b>Find More Phones</b>—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search.</li> <li>• <b>Find More Route Points</b>—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.</li> </ul>
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.

**Table 6-24** Settings for the Application User Configuration Page (continued)

Field	Setting
Groups	The list box displays the groups to which the application user belongs.
Roles	The list box displays the roles that are assigned to the application user.

**Step 4** Select **Save**.

## Creating a New Integration with Cisco Unified Communications Manager

After ensuring that Cisco Unified Communications Manager and Cisco Unity Connection are ready for the integration, do the following procedure to set up the integration and to enter the port settings.


### To Create an Integration

**Step 1** Sign in to Cisco Unity Connection Administration.

**Step 2** If you will use Cisco Unified CM authentication and encryption, do the following substeps. Otherwise, skip to [Step 3](#).

- a. In Cisco Unity Connection Administration, expand **Telephony Integrations**, expand **Security**, then select **SIP Certificate**.
- b. On the SIP Certificates page, select **Add New**.
- c. On the New SIP Certificate page, enter the following settings for the SIP certificate and select **Save**.

**Table 6-25** Settings for the New SIP Certificate Page

Field	Setting
Display Name	Enter a display name for the SIP certificate.
Subject Name	Enter a subject name that matches the X.509 Subject Name of the SIP security profile for the SIP trunk in Cisco Unified CM Administration.   <b>Caution</b> This subject name must match the X.509 Subject Name of the SIP security profile used by Cisco Unified CM. Otherwise, Cisco Unified CM authentication and encryption will fail.

**Step 3** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 4** On the Search Phone Systems page, under Display Name, select the name of the default phone system.

**Step 5** On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.

- Step 6** If you want to use this phone system as the default for TRaP connections so that administrators and users without voicemail boxes can record and playback through the phone in Cisco Unity Connection web applications, check the **Default TRAP Switch** check box. If you want to use another phone system as the default for TRaP connections, uncheck this check box.
- Step 7** Select **Save**.
- Step 8** On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.
- Step 9** On the New Port Group page, enter the applicable settings and select **Save**.

**Table 6-26 Settings for the New Port Group Page**

Field	Setting
Phone System	Select the name of the phone system that you entered in <a href="#">Step 5</a> .
Create From	Select <b>Port Group Template</b> and select <b>SIP</b> in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Authenticate with SIP Server	Check this check box if you want Cisco Unity Connection to authenticate with the Cisco Unified CM server.
Authentication User Name	Enter the name that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Authentication Password	Enter the password that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users will use to contact Cisco Unity Connection and that Cisco Unity Connection will use to register with the Cisco Unified CM server.
SIP Security Profile	Select the SIP security profile that Cisco Unity Connection will use.
SIP Certificate	<i>(Only when a secure TLS port is used)</i> Confirm that the applicable SIP certificate is selected.
Security Mode	<p><i>(Only when a secure TLS port is used)</i> Select the applicable security mode:</p> <ul style="list-style-type: none"> <li>• <b>Authenticated</b>—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an secure TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text.</li> <li>• <b>Encrypted</b>—The integrity and privacy of call-signaling messages will be ensured on this port because they will be connected to Cisco Unified CM through an secure TLS port, and the call-signaling messages will be encrypted.</li> </ul> <p>The Security Mode setting on the Cisco Unity Connection server must match the Device Security Mode setting on the Cisco Unified CM server.</p>
Secure RTP	<i>(Only when a secure TLS port is used)</i> Check this check box so that the media stream (RTP) is encrypted. Uncheck this check box so that the media stream is not encrypted.
SIP Transport Protocol	Select the SIP transport protocol that Cisco Unity Connection will use.

**Table 6-26 Settings for the New Port Group Page (continued)**

Field	Setting
IPv4 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.  You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv6 address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.  You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.  <b>Note</b> IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.
IP Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IP address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.
Port	Enter the TCP port of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.

**Step 10** On the Port Group Basics page, do the following substeps if the Cisco Unified CM cluster has secondary servers, or if you want to add a TFTP server (required for Cisco Unified CM authentication and encryption). Otherwise, skip to [Step 11](#).

- a. On the Edit menu, select **Servers**.
- b. If you want to add a secondary Cisco Unified CM server, on the Edit Servers page, under SIP Servers, select **Add**. Otherwise, skip to [Step 10e](#).
- c. Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

**Table 6-27 Settings for the SIP Servers**

Field	Setting
Order	Enter the order of priority for the Cisco Unified CM server. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IPv4 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv4 address (or host name) of the secondary Cisco Unified CM server.  You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv6 address (or host name) of the secondary Cisco Unified CM server.  You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.  <b>Note</b> IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.

**Table 6-27 Settings for the SIP Servers (continued)**

Field	Setting
IP Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IP address (or host name) of the secondary Cisco Unified CM server.
Port	Enter the IP port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.

- d. If applicable, repeat [Step 10b.](#) and [Step 10c.](#) for an additional Cisco Unified CM server in the Cisco Unified CM cluster.
- e. If you want to add a TFTP server (required for Cisco Unified CM authentication and encryption), under TFTP Servers, select **Add**. Otherwise, skip to [Step 10h.](#)
- f. Enter the following settings for the TFTP server and select **Save**.

**Table 6-28 Settings for the TFTP Servers**

Field	Setting
Order	Enter the order of priority for the TFTP server. The lowest number is the primary TFTP server, the higher numbers are the secondary servers.
IPv4 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv4 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IPv6 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. <b>Note</b> IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.
IP Address or Host Name ( <i>Unity Connection 10.0</i> )	Enter the IP address (or host name) of the TFTP server.

- g. If applicable, repeat [Step 10e.](#) and [Step 10f.](#) for an additional TFTP server.
  - h. On the Edit menu, select **Port Group Basics**.
  - i. On the Port Group Basics page, select **Reset**.
- Step 11** On the Port Group Basics page, in the Related Links drop-down box, select **Add Ports** and select **Go**.
- Step 12** On the New Port page, enter the following settings and select **Save**.

**Table 6-29 Settings for the New Port Page**

Field	Setting
Enabled	Check this check box.
Number of Ports	Enter the number of voice messaging ports that you want to create in this port group. <b>Note</b> For a Cisco Unity Connection cluster, you must enter the total number of voice messaging ports that will be used by all Cisco Unity Connection servers. Each port will later be assigned to a specific Cisco Unity Connection server.
Phone System	Select the name of the phone system that you entered in <a href="#">Step 5</a> .
Port Group	Select the name of the port group that you added in <a href="#">Step 9</a> .
Server	Select the name Cisco Unity Connection server.

- Step 13** On the Search Ports page, select the display name of the first voice messaging port that you created for this phone system integration.



**Note** By default, the display names for the voice messaging ports are composed of the port group display name followed by incrementing numbers.

- Step 14** On the Port Basics page, set the voice messaging port settings as applicable. The fields in the following table are the ones that you can change.

**Table 6-30 Settings for the Voice Messaging Ports**

Field	Considerations
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not answered. Typically, the port is disabled only by the installer during testing.
Server	<i>(For Cisco Unity Connection clusters only)</i> Select the name of the Cisco Unity Connection server that you want to handle this port. Assign an equal number of answering and dial-out voice messaging ports to the Cisco Unity Connection servers so that they equally share the voice messaging traffic.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from unidentified callers or from users.
Perform Message Notification	Check this check box to designate the port for notifying users of messages. Assign Perform Message Notification to the least busy ports.
Send MWI Requests	Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports.
Allow TRAP Connections	Check this check box so that users can use the port for recording and playback through the phone in Cisco Unity Connection web applications. Assign Allow TRAP Connections to the least busy ports.

- Step 15** Select **Save**.

- Step 16** Select **Next**.
- Step 17** Repeat [Step 14](#) through [Step 16](#) for all remaining voice messaging ports for the phone system.
- Step 18** If you will use Cisco Unified CM authentication and encryption, do the following substeps. Otherwise, skip to [Step 20](#).
- In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **Root Certificate**.
  - On the View Root Certificate page, right-click the **Right-click to Save the Certificate as a File** link, and select **Save Target As**.
  - In the Save As dialog box, browse to the location where you want to save the Cisco Unity Connection root certificate as a file.
  - In the File Name field, confirm that the extension is .pem (rather than .htm), and select **Save**.



**Caution** The certificate must be saved as a file with the extension .pem (rather than .htm) or Cisco Unified CM will not recognize the certificate.

- In the Download Complete dialog box, select **Close**.
- Step 19** Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM system integration by doing the following substeps.
- On Cisco Unified CM, sign in to Cisco Unified Operating System Administration page.
  - Navigate to **Security** and select **Certificate Management**.
  - On Certificate List page, select **Upload Certificate/Certificate Chain**.
  - In the Upload Certificate/Certificate Chain window, select CallManager-trust in **Certificate Purpose** field.
  - Browse the file in **Upload File** field and select **Upload**.
- Step 20** If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**. Otherwise, skip to [Step 24](#).
- Step 21** On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.
- Step 22** On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

**Table 6-31 Settings for the Phone System Trunk**

Field	Setting
From Phone System	Select the display name of the phone system that you are creating a trunk for.
To Phone System	Select the display name of the previously existing phone system that the trunk will connect to.
Trunk Access Code	Enter the extra digits that Cisco Unity Connection must dial to transfer calls through the gateway to extensions on the previously existing phone system.

- Step 23** Repeat [Step 21](#) and [Step 22](#) for all remaining phone system trunks that you want to create.
- Step 24** In the Related Links drop-down list, select **Check Telephony Configuration** and select **Go** to confirm the phone system integration settings.



If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.

**Step 25** In the Task Execution Results window, select **Close**.

---

