



# Cisco Unified Communications Manager 6.x SCCP Integration Guide for Cisco Unity Connection 1.2

---

*Revised November 21, 2007*

This document provides instructions for integrating Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) with Cisco Unity Connection by Skinny Call Control Protocol (SCCP).

Cisco Unity Connection supports an SCCP integration when Cisco Unified CM has only SCCP phones or has both SCCP and SIP phones.



**Note**

---

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

---

## Integration Tasks

Before doing the following tasks to integrate Cisco Unity Connection with the Cisco Unified CM phone system, 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*.

The following task lists describe the process for creating and changing integrations.

## Task List to Create the Integration by SCCP

Use the following task list to set up a new integration with the Cisco Unified CM phone system.

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 2](#).
2. Plan how the voice messaging ports will be used by Cisco Unity Connection. See the [“Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection” section on page 5](#).



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

3. Program Cisco Unified CM. See the “[Programming the Cisco Unified Communications Manager Phone System](#)” section on page 7.
4. Create the integration. See the “[Creating a New Integration with the Cisco Unified Communications Manager Phone System](#)” section on page 17.




---

**Note** An additional Cisco Unified CM cluster can be added by creating a new phone system integration through the Phone System Integration Wizard. Each Cisco Unified CM cluster is a separate phone system integration.

---

5. Test the integration. See the “[Testing the Integration](#)” section on page 25.
6. If this integration is a second or subsequent integration, add the applicable new user templates for the new phone system. See the [\(Multiple Integrations Only\) Adding New User Templates](#), page 29.

## Task List to Change the Number of Voice Messaging Ports

Use the following task list to change the number of voice messaging ports for an integration after it has been created.

1. Change the number of voice messaging ports in Cisco Unified CM Administration and in Cisco Unity Connection Administration. See the “[Changing the Number of Voice Messaging Ports](#)” section on page 29.

## Task List to Add a Cisco Unified Communications Manager Express Server to a Cisco Unified Communications Manager Cluster

Use the following task list to add a Cisco Unified CM Express server to a Cisco Unified CM cluster.

1. Confirm that the Cisco Unified CM Express server meets the requirements for integrating with Cisco Unity Connection. Refer to the applicable Cisco Unified CM Express integration guide at [http://www.cisco.com/en/US/products/ps6509/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html).
2. Add the Cisco Unified CM Express server to the port group for the Cisco Unified CM phone system integration. See “[Adding a Cisco Unified Communications Manager Express Server to a Cisco Unified Communications Manager Phone System Integration](#)” section on page 32.
3. If needed, add voice messaging ports. See the “[Changing the Number of Voice Messaging Ports](#)” section on page 29.

## Requirements

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

### Phone System

- A Cisco IP telephony applications server consisting of Cisco Unified CM 6.x, running on a Cisco Media Convergence Server (MCS) or customer-provided server meeting approved Cisco configuration standards.

For details on compatible versions of Cisco Unified CM, refer to the *SCCP 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).

- The following phones or combinations of phones for the Cisco Unified CM extensions:
  - Only IP phones for the Cisco Unified CM extensions.
  - Both IP phones and SIP phones for the Cisco Unified CM extensions without a media termination point (MTP) on the Cisco Unified CM server.
  - Both IP phones and SIP phones for the Cisco Unified CM extensions with a media termination point (MTP) on the Cisco Unified CM server.
- 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, refer to the *SCCP 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).
- The applicable Cisco Unity-CM TSP, installed. For details on compatible versions of the TSP, refer to the *SCCP 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).
- A license that enables the applicable number of voice messaging ports.

## Integration Description

The Cisco Unified Communications Manager integration makes connections through a LAN or WAN. A gateway provides connections to the PSTN.

## Call Information

The phone system sends the following information with forwarded calls:

- The extension of the called party
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the system uses caller ID)
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls)

Cisco Unity Connection uses this information to answer the call appropriately. For example, a call forwarded to Cisco Unity Connection is answered with the personal greeting of the user. If the phone system routes the call to Cisco Unity Connection without this information, Cisco Unity Connection answers with the opening greeting.

## Integration Functionality

The Cisco Unified CM integration with Cisco Unity Connection provides the following features:

- Call forward to personal greeting
- Call forward to busy greeting
- Caller ID
- Easy message access (a user can retrieve messages without entering an ID; Cisco Unity Connection identifies a user based on the extension from which the call originated; a password may be required)
- Identified user messaging (Cisco Unity Connection automatically identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated)
- Message waiting indication (MWI)

The functionality of this integration may be affected by the issues described below.

### Use of Cisco Unified Survivable Remote Site Telephony (SRST) Router

When a Cisco Unified Survivable Remote Site Telephony (SRST) router is part of the network and the Cisco Unified SRST router takes over call processing functions from Cisco Unified CM (for example, because the WAN link is down), phones at a branch office can continue to function. In this situation, however, the integration features have the following limitations:

- **Call forward to busy greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Cisco Unity Connection, the busy greeting cannot play.
- **Call forward to internal greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Cisco Unity Connection, the internal greeting cannot play. Because the PSTN provides the calling number of the FXO line, the caller is not identified as a user.
- **Call transfers**—Because an access code is needed to reach the PSTN, call transfers from Cisco Unity Connection to a branch office will fail.
- **Identified user messaging**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a user at a branch office leaves a message or forwards a call, the user is not identified. The caller appears as an unidentified caller.
- **Message waiting indication**—MWIs are not updated on branch office phones, so MWIs will not correctly reflect when new messages arrive or when all messages have been listened to. We recommend resynchronizing MWIs after the WAN link is reestablished.
- **Routing rules**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call arrives from a branch office to Cisco Unity Connection (either a direct or forwarded call), routing rules will fail.

When the Cisco Unified SRST router uses PRI/BRI connections, the caller ID for calls from a branch office to Cisco Unity Connection may be the full number (exchange plus extension) provided by the PSTN and therefore may not match the extension of the Cisco Unity Connection user. If this is the case, you can let Cisco Unity Connection recognize the caller ID by using alternate extensions.

Redirected Dialed Number Information Service (RDNIS) needs to be supported when using SRST.

For information on setting up Cisco Unified SRST routers, refer to the “Integrating Voice Mail with Cisco Unified SRST” section of the *Cisco Unified SRST System Administrator Guide* at [http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html).

### Impact of Non-Delivery of RDNIS on Voice Mail Calls Routed via AAR

RDNIS needs to be supported when using Automated Alternate Routing (AAR).

AAR can route calls over the PSTN when the WAN is oversubscribed. However, when calls are rerouted over the PSTN, RDNIS can be affected. Incorrect RDNIS information can affect voice mail calls that are rerouted over the PSTN by AAR when Cisco Unity Connection is remote from its messaging clients. If the RDNIS information is not correct, the call will not reach the voice mail box of the dialed user but will instead receive the automated attendant prompt, and the caller might be asked to reenter the extension number of the party they wish to reach. This behavior is primarily an issue when the telephone carrier is unable to ensure RDNIS across the network. There are numerous reasons why the carrier might not be able to ensure that RDNIS is properly sent. Check with your carrier to determine whether it provides guaranteed RDNIS delivery end-to-end for your circuits. The alternative to using AAR for oversubscribed WANs is simply to let callers hear reorder tone in an oversubscribed condition.

## Integrations with Multiple Phone Systems

Cisco Unity Connection can be integrated with multiple phone systems at one time. For information on and instructions for integrating Cisco Unity Connection with multiple phone systems, refer to the *Multiple Phone System Integration Guide* at [http://www.cisco.com/en/US/products/ps6509/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html).

## Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection

Before programming the phone system, you need to plan how the voice messaging ports will be used by Cisco Unity Connection. The following considerations will affect the programming for the phone system (for example, setting up the hunt group or call forwarding for the voice messaging ports):

- The number of voice messaging ports installed.
- The number of voice messaging ports that will answer calls.
- The number of voice messaging ports that will only dial out, for example, to send message notification, to set message waiting indicators (MWIs), and to make telephone record and playback (TRAP) connections.

The following table describes the voice messaging port settings in Cisco Unity Connection that can be set on Telephony Integrations > Port of Cisco Unity Connection Administration.

**Table 1**      **Settings for the Voice 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.
Extension	Enter the extension for the port as assigned on the phone system.
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.

**Table 1**      **Settings for the Voice Ports (continued)**

Field	Considerations
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.
Outgoing Hunt Order	Enter the priority order in which Cisco Unity Connection will use the ports when dialing out (for example, if the Perform Message Notification, Send MWI Requests, or Allow TRAP Connections check box is checked). The highest numbers are used first. However, when multiple ports have the same Outgoing Hunt Order number, Cisco Unity Connection will use the port that has been idle the longest.
Security Mode	Click the applicable security mode: <ul style="list-style-type: none"> <li>• <b>Non-secure</b>—The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream will not be encrypted.</li> <li>• <b>Authenticated</b>—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. In addition, the media stream will not be encrypted.</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 authenticated TLS port, and the call-signaling messages will be encrypted. In addition, the media stream will be encrypted.</li> </ul>

### The Number of Voice Messaging Ports to Install

The number of voice messaging ports to install depends on numerous factors, including:

- The number of calls Cisco Unity Connection will answer when call traffic is at its peak.
- The expected length of each message that callers will record and that users will listen to.
- The number of users.
- The number of ports that will be set to dial out only.
- The number of calls made for message notification.
- The number of MWIs that will be activated when call traffic is at its peak.
- The number of TRAP connections needed when call traffic is at its peak. (TRAP connections are used by Cisco Unity Connection web applications to play back and record over the phone.)
- The number of calls that will use the automated attendant and call handlers when call traffic is at its peak.

It is best to install only the number of voice messaging ports that are needed so that system resources are not allocated to unused ports.

### The Number of Voice Messaging Ports That Will Answer Calls

The calls that the voice messaging ports answer can be incoming calls from unidentified callers or from users. Typically, the voice messaging ports that answer calls are the busiest.

You can set voice messaging ports to both answer calls and to dial out (for example, to send message notifications). However, when the voice messaging ports perform more than one function and are very active (for example, answering many calls), the other functions may be delayed until the voice messaging port is free (for example, message notifications cannot be sent until there are fewer calls to answer). For best performance, dedicate certain voice messaging ports for only answering incoming calls, and dedicate other ports for only dialing out. Separating these port functions eliminates the possibility of a collision, in which an incoming call arrives on a port at the same time that Cisco Unity Connection takes the port off-hook to dial out.

### The Number of Voice Messaging Ports That Will Only Dial Out, and Not Answer Calls

Ports that will only dial out and will not answer calls can do one or more of the following:

- Notify users by phone, pager, or e-mail of messages that have arrived.
- Turn MWIs on and off for user extensions.
- Make a TRAP connection so that users can use the phone as a recording and playback device in Cisco Unity Connection web applications.

Typically, these voice messaging ports are the least busy ports.



#### Caution

In programming the phone system, do not send calls to voice messaging ports in Cisco Unity Connection that cannot answer calls (voice messaging ports that are not set to Answer Calls). For example, if a voice messaging port is set only to Send MWI Requests, do not send calls to it.

### Preparing for Programming the Phone System

Record your decisions about the voice messaging ports to guide you in programming the phone system.

# Programming the Cisco Unified Communications Manager Phone System

Do the following procedures in the order given.

## To Add Partitions and a Calling Search Space to Contain the Voice Mail Ports

- 
- Step 1** In Cisco Unified CM Administration, click **Call Routing > Class of Control > Partition**.
- Step 2** On the Find and List Partitions page, click **Add New**.
- Step 3** On the Partition Configuration page, enter the name and description you want for the partition that will contain all voice mail port directory numbers. For example, enter “VMRestrictedPT, Partition for voice mail port directory numbers.”
- Step 4** Click **Save**.
- Step 5** Click **Add New**.
- Step 6** Enter the name and description you want for the partition that will contain the hunt pilot, which will be the voice mail pilot number. For example, enter “VMPilotNumberPT, Partition for the voice mail pilot number.”

- Step 7** Click **Save**.
- Step 8** Click **Call Routing > Class of Control > Calling Search Space**.
- Step 9** On the Find and List Calling Search Spaces page, click **Add New**.
- Step 10** On the Calling Search Space Configuration page, in the Name field, enter a name for the calling search space that will include the partition created in [Step 2](#) through [Step 4](#). For example, enter “VMRestrictedCSS.”
- Step 11** Optionally, in the Description field, enter a description of the calling search space. For example, enter “Voice mail port directory numbers.”
- Step 12** In the Available Partitions list, click the name of the partition created in [Step 2](#) through [Step 4](#). For example, click “VMRestrictedPT.”
- Step 13** Click the down arrow below the Available Partitions list.  
The name of the partition appears in the Selected Partitions list.
- Step 14** Click **Save**.
- Step 15** In the Related Links field, click **Back to Find/List** and click **Go**.
- Step 16** On the Find and List Calling Search Spaces page, click **Find**.
- Step 17** Click the name of the calling search space that is used by user phones.
- Step 18** On the Calling Search Space Configuration page, in the Available Partitions list, click the name of the partition created in [Step 5](#) through [Step 7](#). For example, click “VMPilotNumberPT.”




---

**Caution** If the partition that contains the hunt pilot (which will be the voice mail pilot number) is not in the calling search space that is used by user phones, the phones will not be able to dial the Cisco Unity Connection server.

---

- Step 19** Click the down arrow below the Available Partition list.  
The name of the partition appears in the Selected Partitions list.
- Step 20** Click **Save**.
- Step 21** Repeat [Step 17](#) through [Step 20](#) for each remaining calling search space that needs to access Cisco Unity Connection.

---

### To Add a Device Pool for the Voice Mail Ports

---

- Step 1** In Cisco Unified CM Administration, click **System > Device Pool**.
- Step 2** On the Find and List Device Pools page, click **Add New**.
- Step 3** On the Device Pool Configuration page, enter the following device pool settings.

**Table 2** Settings for the Device Pool Configuration Page

Field	Setting
Device Pool Name	Enter <b>Cisco Unity Connection Voice Mail Ports</b> or other description for this device pool.
Cisco Unified Communications Manager Group	Click the Cisco Unified Communications Manager group to assign to the voice mail ports in this device pool.
Date/Time Group	Click the date/time group to assign to the voice mail ports in this device pool.
Region	Click the Cisco Unified CM region to assign to the voice mail ports in this device pool.
SRST Reference	If applicable, click the survivable remote site telephony (SRST) reference to assign to the voice mail ports in this device pool.

**Step 4** Click **Save**.

In the following procedure, add a voice mail port to Cisco Unified CM for each voice mail port that you will connect to Cisco Unity Connection.

#### To Add Voice Mail Ports to Cisco Unified CM

**Step 1** In Cisco Unified CM Administration, click **Voice Mail > Cisco Voice Mail Port Wizard**.

**Step 2** On the What Would You Like to Do page, click **Create a New Cisco Voice Mail Server and Add Ports to It**, and click **Next**.

**Step 3** On the Cisco Voice Mail Server page, the name of the voice mail server appears. We recommend that you accept the default name for the voice mail server. If you must use a different name, however, the name must have no more than nine characters.

The voice mail server name must match the Device Name Prefix field in Cisco Unity Connection on the Port Group Basics page for the voice messaging ports.

**Step 4** Click **Next**.

**Step 5** On the Cisco Voice Mail Ports page, click the number of voice mail ports that you want to add (which must not be more voice mail ports than the Cisco Unity Connection license enables), then click **Next**.

If you will integrate Cisco Unity Connection with multiple clusters of Cisco Unified CM, the number you enter here cannot bring the total number of ports on all clusters integrated with Cisco Unity Connection to more than the number of ports enabled by the Cisco Unity Connection license.

**Step 6** On the Cisco Voice Mail Device Information page, enter the following voice mail device settings.

**Table 3** Settings for the Cisco Voice Mail Device Information Page

Field	Setting
Description	Enter <b>Cisco Voice Mail Port</b> or another description for the voice mail device.
Device Pool	Click the name of the device pool you created for the voice mail ports. For example, click Cisco Unity Connection Voice Mail Ports.

**Table 3 Settings for the Cisco Voice Mail Device Information Page (continued)**

Field	Setting
Calling Search Space	<p>Click the name of a calling search space that allows calls to the user phones and any required network devices.</p> <p>This calling search space must include partitions that contain all devices Cisco Unity Connection needs to access (for example, during call transfers, message notifications, and MWI activations).</p>
AAR Calling Search Space	Accept the default of <b>None</b> .
Location	Click <b>Hub_None</b> .
Device Security Mode	<p>Click the security mode that you want to use for the voice mail ports. For details on the settings for Cisco Unified CM authentication and encryption of the voice mail ports, see the <a href="#">“Appendix: Cisco Unified Communications Manager Authentication and Encryption of Cisco Unity Connection Voice Messaging Ports”</a> section on page 33.</p>

**Step 7** Click **Next**.

**Step 8** On the Cisco Voice Mail Directory Numbers page, enter the following voice mail directory number settings.

**Table 4 Settings for the Cisco Voice Mail Directory Numbers Page**

Field	Setting
Beginning Directory Number	Enter the extension number of the first voice mail port.
Partition	Click the name of the partition that you set up for all voice mail port directory numbers. For example, click “VMRestrictedPT.”
Calling Search Space	<p>Click the name of a calling search space that you set up to contain the partition with all voice mail port directory numbers, as set in <a href="#">Step 9</a> of the <a href="#">“To Add Partitions and a Calling Search Space to Contain the Voice Mail Ports”</a> procedure on page 7. For example, click “VMRestrictedCSS.”</p> <p>Because this calling search space is not used by user phones, users are not able to dial the voice mail ports. However, users can dial the voice mail pilot number.</p>
AAR Group	<p>Click the automated alternate routing (AAR) group for the voice mail ports. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If you click <b>None</b>, no rerouting of blocked calls will be attempted.</p>
Internal Caller ID Display	<p>Accept the default of <b>VoiceMail</b>.</p> <p>This text appears on the phone when the pilot number is dialed.</p>

**Table 4** Settings for the Cisco Voice Mail Directory Numbers Page (continued)

Field	Setting
Internal Caller ID Display (ASCII Format)	Accept the default of <b>VoiceMail</b> . This text appears on the phone when the pilot number is dialed.
External Number Mask	Leave this field blank, or specify the mask used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information, and enter <b>X</b> for each digit in the directory number of the device.

**Step 9** Click **Next**.

**Step 10** On the Do You Want to Add These Directory Numbers to a Line Group page, click **No, I Will Add Them Later**, and click **Next**.

**Step 11** On the Ready to Add Cisco Voice Mail Ports page, confirm that the settings for the voice mail ports are correct, and click **Finish**.

If the settings are not correct, click **Back** and enter the correct settings.

#### To Add Voice Mail Ports to Line Groups

**Step 1** In Cisco Unified CM Administration, click **Call Routing > Route/Hunt > Line Group**.

**Step 2** On the Find and List Line Groups page, click **Add New**.

This line group will contain directory numbers for voice mail ports that will answer calls. Directory numbers for voice mail ports that will only dial out (for example, to set MWIs) must not be included in this line group.

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

**Table 5** Settings for the Line Group Configuration Page for Answering Ports

Field	Setting
Line Group Name	Enter <b>Cisco Unity Connection Answering Ports</b> or another unique name for line groups.
RNA Reversion Timeout	Accept the default of <b>10</b> .
Distribution Algorithm	Click <b>Top Down</b> .
No Answer	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .
Busy	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .
Not Available	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .

**Step 4** Under Line Group Member Information, in the Partition list, click the name of the partition that you set up for all voice mail port directory numbers. For example, click “VMRestrictedPT.”

**Step 5** Click **Find**.

**Step 6** In the Available DN/Route Partition list, click the first directory number of a voice mail port that will answer calls, and click **Add to Line Group**.



**Caution** The directory numbers in the Selected DN/Route Partition list must appear in numerical sequence with the lowest number on top. Otherwise, the integration will not function correctly.

**Step 7** Repeat [Step 6](#) for all remaining directory numbers of voice mail ports that will answer calls.



**Caution** Do not include directory numbers of voice mail ports that will only dial out (for example, to set MWIs). Otherwise, the integration will not function correctly.

**Step 8** Click **Save**.

**Step 9** If you will have voice mail ports that will only dial out (will not answer calls), do [Step 10](#) through [Step 16](#).

Otherwise, skip the remaining steps in this procedure and continue on to the [“To Add the Line Group to a Hunt List” procedure on page 13](#).

**Step 10** Click **Add New**.

This line group will contain directory numbers for voice mail ports that will only dial out. Directory numbers for voice mail ports that answer calls must not be included in this line group.

**Step 11** On the Line Group Configuration page, enter the following settings.

**Table 6** Settings for the Line Group Configuration Page for Dial-Out Ports

Field	Setting
Line Group Name	Enter <b>Cisco Unity Connection Dial-Out Ports</b> or another unique name.
RNA Reversion Timeout	Accept the default of <b>10</b> .
Distribution Algorithm	Click <b>Top Down</b> .
No Answer	Click <b>Stop Hunting</b> .
Busy	Click <b>Stop Hunting</b> .
Not Available	Click <b>Stop Hunting</b> .

**Step 12** Under Line Group Member Information, in the Partition list, click the name of the partition that you set up for all voice mail port directory numbers. For example, click “VMRestrictedPT.”

**Step 13** Click **Find**.

**Step 14** In the Available DN/Route Partition list, click the first directory number of a voice mail port that will only dial out, and click **Add to Line Group**.



**Caution** The directory numbers in the Selected DN/Route Partition list must appear in numerical sequence with the lowest number on top. Otherwise, the integration will not function correctly.

**Step 15** Repeat [Step 14](#) for all remaining voice mail ports that will only dial out.



**Caution** Do not include directory numbers of voice mail ports that will answer calls. Otherwise, the integration will not function correctly.

**Step 16** Click **Save**.

---

### To Add the Line Group to a Hunt List

---

**Step 1** In Cisco Unified CM Administration, click **Call Routing > Route/Hunt > Hunt List**.

**Step 2** On the Find and List Hunt Lists page, click **Add New**.

**Step 3** On the Hunt List Configuration page, enter the following settings for the hunt list.

**Table 7** *Settings for the Hunt List Configuration Page for Answering Ports*

Field	Setting
Name	Enter <b>Cisco Unity Connection Answering Ports</b> or another unique name for the hunt list.
Description	Enter <b>Cisco Unity Connection ports that answer calls</b> or another description.
Cisco Unified Communications Manager Group	Click <b>Default</b> or the name of the Cisco Unified Communications Manager group that you are using.
Enable This Hunt List	Check this check box.
For Voice Mail Usage	Check this check box.

**Step 4** Click **Save**.

**Step 5** Under Hunt List Member Information, click **Add Line Group**.

**Step 6** On the Hunt List Detail Configuration page, in the Line Group list, click the line group you created for the directory numbers of voice mail ports that will answer calls, then click **Save**.



**Caution** In the hunt list, do not include line groups with voice mail ports that Cisco Unity Connection will use to dial out. Otherwise, the integration will not function correctly.

**Step 7** When alerted that the line group has been inserted, click **OK**.

**Step 8** On the Hunt List Configuration page, click **Reset**.

**Step 9** When asked to confirm resetting the hunt list, click **Reset**.

**Step 10** When alerted that the hunt list has been reset, click **Close**.

---

**To Add the Hunt List to a Hunt Pilot Number**

- Step 1** In Cisco Unified CM Administration, click **Call Routing > Route/Hunt > Hunt Pilot**.
- Step 2** On the Find and List Hunt Pilots page, click **Add New**.
- Step 3** On the Hunt Pilot Configuration page, enter the following settings for the hunt pilot.

**Table 8 Settings for Hunt Pilot Configuration Page**

Field	Setting
Hunt Pilot	Enter the hunt pilot number for the voice mail ports. The hunt pilot number must be different from the extension numbers of the voice mail ports.  The hunt pilot number is the extension number that users enter to listen to their voice messages.
Partition	Click the name of the partition that you set up for the voice mail pilot number. For example, click “VMPilotNumberPT.”
Description	Enter <b>Connection Hunt Pilot</b> or another description.
Numbering Plan	Accept the default setting, or click the numbering plan that you have set up for your system.
Route Filter	Click <b>None</b> , or click the name of the route filter that you set up for your system.
MLPP Precedence	Accept the default setting, or click another setting.
Hunt List	Click the hunt list of voice mail ports that answer calls, which you set up in the <a href="#">“To Add the Line Group to a Hunt List” procedure on page 13</a> .
Route Option	Click <b>Route This Pattern</b> .
Provide Outside Dial Tone	Uncheck the check box.

- Step 4** Click **Save**.

**To Specify MWI Directory Numbers**

- Step 1** In Cisco Unified CM Administration, click **Voice Mail > Message Waiting**.
- Step 2** On the Find and List Message Waiting Numbers page, click **Add New**.
- Step 3** On the Message Waiting Configuration page, enter the following settings for turning MWIs on.

**Table 9 Settings for Turning MWIs On**

Field	Setting
Directory Number	Enter the unique extension that turns MWIs on.
Partition	Click the name of the partition that you set up for the voice mail pilot number. For example, click “VMPilotNumberPT.”
Description	Enter <b>DN to turn MWIs on</b> or another description.

**Table 9** Settings for Turning MWIs On (continued)

Field	Setting
Message Waiting Indicator	Click <b>On</b> .
Calling Search Space	Click a calling search space that is used by user phones.

- Step 4** Click **Save**.
- Step 5** Click **Add New**.
- Step 6** Enter the following settings for turning MWIs off.

**Table 10** Settings for Turning MWIs Off

Field	Setting
Directory Number	Enter the unique extension that turns MWIs off.
Partition	Click the name of the partition that you set up for the voice mail pilot number. For example, click “VMPilotNumberPT.”
Description	Enter <b>DN to turn MWIs off</b> or another description.
Message Waiting Indicator	Click <b>Off</b> .
Calling Search Space	Click a calling search space that is used by user phones.

- Step 7** Click **Save**.

In the following procedure, you will add the voice mail pilot number, which is the extension that you dial to listen to your voice messages. Your Cisco IP phone automatically dials the voice mail pilot number when you press the Messages button.

#### To Add a Voice Mail Pilot Number for the Voice Mail Ports

- Step 1** In Cisco Unified CM Administration, click **Voice Mail > Voice Mail Pilot**.
- Step 2** On the Find and List Voice Mail Pilots page, click **Add New**.
- Step 3** On the Voice Mail Pilot Configuration page, enter the following voice mail pilot number settings.

**Table 11** 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 be the same as the hunt pilot number that you entered when adding voice mail ports earlier.
Calling Search Space	Click the calling search space that includes partitions containing the user phones and the partition you set up for the voice mail pilot number.
Description	Enter <b>Cisco 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** Click **Save**.

**To Set Up the Voice Mail Profile**

**Step 1** In Cisco Unified CM Administration, click **Voice Mail > Voice Mail Profile**.

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

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

**Table 12 Settings for the Voice Mail Profile Configuration Page**

Field	Setting
Voice Mail Profile Name	Enter a name to identify the voice mail profile.
Description	Enter <b>Cisco Unity Connection Profile</b> or another description.
Voice Mail Pilot	Click one of the following: <ul style="list-style-type: none"> <li>• The applicable voice mail pilot number that you defined on the Voice Mail Pilot Configuration page</li> <li>• <b>Use Default</b></li> </ul>
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** Click **Save**.

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

**Step 1** In Cisco Unified CM Administration, click **System > Service Parameters**.

**Step 2** On the Service Parameters Configuration page, in the Server field, click the name of the Cisco Unified CM server.

**Step 3** In the Service list, click 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, click **True**.

When this parameter is set to True, Cisco Unified CM uses any configured translation patterns to convert voice mail extensions into directory numbers when turning on or off an MWI.

- Step 6** If you changed any settings, click **Save**. Then shut down and restart the Cisco Unified CM server.

## Creating a New Integration with the Cisco Unified Communications Manager Phone System

After ensuring that the Cisco Unified CM phone system 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** Log on to Cisco Unity Connection Administration.
- Step 2** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 3** On the Search Phone Systems page, on the Phone System menu, click **New Phone System**. The Phone System Integration Wizard appears.
- Step 4** On the Select Phone System Manufacturer page, in the Manufacturer field, click **Cisco Systems** and click **Next**.
- Step 5** On the Select Phone System Model page, in the Model field, click **Cisco Unified CallManager** and click **Next**.
- Step 6** On the Set Up Phone System page, in the Phone System Name field, accept the default name or enter the descriptive name that you want, and click **Next**.
- Step 7** On the Select Port Group Template page, in the Port Group Template field, click **SCCP - Skinny Client Control Protocol** and click **Next**.
- Step 8** On the Set Up Port Group page, enter the following settings and click **Next**.

**Table 13** Settings for the Set Up Port Group Page


Field	Setting
Port Group Name	<the display name for the port group; accept the default name, which is composed of the phone system display name followed by an incrementing number, or enter another descriptive name>
Device Name Prefix	<the prefix that Cisco Unified CM adds to the device name for voice ports; this prefix must match the prefix used by Cisco Unified CM>
MWI On Extension	<the extension that you specified in Cisco Unified CM Administration for turning MWIs on>
MWI Off Extension	<the extension that you specified in Cisco Unified CM Administration for turning MWIs off>
Security Mode	<the Cisco Unified CM security mode that you want to use for the voice messaging ports in this port group>
Number of Ports	<the number of voice messaging ports that you want to create in this port group>
IP Address or Host Name	<the IP address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection>

**Table 13 Settings for the Set Up Port Group Page (continued)**

Field	Setting
Test Address	Click this button to test the IP address that you entered. The results of the test appear in the field to the right of the button.
Port	<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>
TLS Port	<the TLS port of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection; we recommend that you use the default setting>
Server Type	<b>Cisco CallManager</b>

- Step 9** On the Confirm Phone System Settings page, confirm the settings that you have entered and click **Finish**.
- Step 10** On the Phone System Creation Summary page, click **Close**.
- Step 11** If Cisco Unity Connection does not connect to an AXL server, skip to [Step 17](#). Otherwise, on the Search Phone Systems page, click the display name of the phone system that you created in [Step 9](#).
- Step 12** On the Phone System Basics page, in the Edit menu, click **Cisco CallManager AXL Servers**.

Connecting to an AXL server is needed when Cisco Unity Connection must have access to the Cisco Unified CM database for importing Cisco Unified CM users and for changing certain phone settings for users of Cisco Unity Connection personal call transfer rules.

 **Caution** If you plan to import Cisco Unified CM users, confirm that the Primary Extension field on the End User Configuration page for each user is filled in. Otherwise, the search will not find any users to select for importing.

- Step 13** Under AXL Servers, click **Add New**.
- Step 14** Enter the following settings for the AXL server and click **Save**.

**Table 14 Settings for the AXL Servers**

Field	Setting
Order	<the order of priority for the AXL server; the lowest number is the primary AXL server, the higher numbers are the secondary servers>
IP Address or Host Name	<the IP address (or host name) of the AXL server>
Port	<the AXL server port that Cisco Unity Connection connects to; this setting must match the port that the AXL server will use>  The port number is typically 8443.

- Step 15** Repeat [Step 13](#) and [Step 14](#) for all remaining AXL servers.
- Step 16** Under AXL Server Settings, enter the following settings and click **Save**.

**Table 15**      **Settings for the AXL Settings**

Field	Setting
User Name	<the user name that Cisco Unity Connection will use to log on to the AXL server>
Password	<the password that Cisco Unity Connection will use to log on to the AXL server>
Cisco CallManager Version	<b>5.0 or Greater (SSL)</b> The AXL port must be an SSL-enabled port (typically port 8443).



**Note** After the changes to this page are saved, you can click **Test** (next to the AXL server port number) to verify the connection to the AXL server.

**Step 17** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.

**Step 18** On the Search Port Groups page, click the display name of the port group that you created with the phone system integration in [Step 9](#).



**Note** By default, the display name for a port group is composed of the phone system display name followed by an incrementing number.

**Step 19** On the Port Group Basics page, on the Edit menu, click **Servers**.

**Step 20** On the Edit Servers page, do the following substeps if the Cisco Unified CM cluster has secondary servers. Otherwise, skip to [Step 21](#).

- a. Under Cisco CallManager Servers, click **Add**.
- b. Enter the following settings for the secondary Cisco Unified CM server and click **Save**.

**Table 16**      **Settings for the Cisco Unified CM Server**

Field	Setting
Order	<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>
IP Address or Host Name	<the IP address (or host name) of the secondary Cisco Unified CM server>
Port	<the TCP 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	<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>
Server Type	<b>Cisco CallManager</b>



**Note** You can click **Ping** to verify the IP address (or host name) of the Cisco Unified CM server.

c. Repeat [Step 20a.](#) and [Step 20b.](#) for all remaining Cisco Unified CM servers in the cluster.

**Step 21** Do the following substeps if the Cisco Unified CM cluster uses authentication or encryption for the voice messaging ports. Otherwise, skip to [Step 22.](#)

a. Under TFTP Servers, click **Add.**

b. Enter the following settings for the TFTP server and click **Save.**

**Table 17 Settings for the TFTP Server**

Field	Setting
Order	<the order of priority for the TFTP server; the lowest number is the primary TFTP server, the higher numbers are the secondary servers>
IP Address or Host Name	<the IP address (or host name) of the TFTP server>



**Note** You can click **Ping** to verify the IP address (or host name) of the TFTP server.

c. Repeat [Step 21a.](#) and [Step 21b.](#) for all remaining TFTP servers in the cluster.

**Step 22** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port.**

**Step 23** On the Search Ports page, click 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 24** 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 18 Settings for the Voice 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.
Extension	Enter the extension for the port as assigned on the phone system.
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.

**Table 18**      *Settings for the Voice Ports (continued)*

Field	Considerations
Outgoing Hunt Order	Enter the priority order in which Cisco Unity Connection will use the ports when dialing out (for example, if the Perform Message Notification, Send MWI Requests, or Allow TRAP Connections check box is checked). The highest numbers are used first. However, when multiple ports have the same Outgoing Hunt Order number, Cisco Unity Connection will use the port that has been idle the longest.
Security Mode	Click the applicable security mode: <ul style="list-style-type: none"> <li>• <b>Non-secure</b>—The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream will not be encrypted.</li> <li>• <b>Authenticated</b>—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. In addition, the media stream will not be encrypted.</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 authenticated TLS port, and the call-signaling messages will be encrypted. In addition, the media stream will be encrypted.</li> </ul>

- Step 25** Click **Save**.
- Step 26** Click **Next**.
- Step 27** Repeat [Step 24](#) through [Step 26](#) for all remaining voice messaging ports for the phone system.
- Step 28** If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Trunk**. Otherwise, skip to [Step 32](#).
- Step 29** On the Search Phone System Trunks page, on the Phone System Trunk menu, click **New Phone System Trunk**.
- Step 30** On the New Phone System Trunk page, enter the following settings for the phone system trunk and click **Save**.

**Table 19**      *Settings for the Phone System Trunk*

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

- Step 31** Repeat [Step 29](#) and [Step 30](#) for all remaining phone system trunks that you want to create.
- Step 32** If prompted to restart Cisco Unity Connection, in the Windows task bar, right-click the **Cisco Unity Connection** icon and click **Restart > Voice Processing Server Role**.
- Step 33** When prompted to confirm stopping the Voice Processing server role, click **Yes**.

**Step 34** In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **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 35** In the Task Execution Results window, click **Close**.

**Step 36** If you do not want to set up for Cisco Unified CM authentication and encryption, log off Cisco Unity Connection Administration, skip the remaining procedures, and continue with the [“Testing the Integration”](#) section on page 25.

If you want to set up for Cisco Unified CM authentication and encryption, continue with the [“Setting Up Cisco Unified Communications Manager Authentication and Encryption with Cisco Unity Connection”](#) below.

## Setting Up Cisco Unified Communications Manager Authentication and Encryption with Cisco Unity Connection

If you are not setting up Cisco Unified CM authentication and encryption, skip to the [“Testing the Integration”](#) section on page 25.

If you are setting up Cisco Unified CM authentication and encryption, do the following procedures.

For additional information about authentication and encryption with Cisco Unified CM and Cisco Unity Connection, see the [“Appendix: Cisco Unified Communications Manager Authentication and Encryption of Cisco Unity Connection Voice Messaging Ports”](#) section on page 33.



### Caution

The Cisco Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM will reject the Cisco Unity Connection voice messaging ports until the Cisco Unified CM system clock has passed the time stamp in the Cisco Unity Connection device certificates.

### To Ensure That the Tftp.exe File Is Present on Cisco Unity Connection Server

**Step 1** On the Cisco Unity Connection server, determine whether the computer is one of the following models:

- MCS-7825H-2.2-ECS1
- MCS-7825H-3.0-ECS1
- MCS-7835H-2.4-ECS1
- MCS-7835H-3.4-ECS1
- MCS-7845H-2.4-ECS1
- MCS-7845H-3.0-ECS1
- MCS-7815I-3.0-ECS1
- MCS-7815-I1-ECS1
- MCS-7815-I1-UC1
- MCS-7825-I1-ECS1

- MCS-7825-I1-UC1
- MCS-7835-I1-ECS1
- MCS-7835-I1-UC1
- MCS-7845-I1-ECS1
- MCS-7845-I1-UC1

**Step 2** If the computer is not one of the computer models listed above, skip the remaining steps in this procedure and continue to the [“To Enable Cisco Unified CM Authentication and Encryption for Cisco Unity Connection Voice Messaging Ports”](#) procedure on page 23.

Otherwise, on the Start menu, click **Run**.

**Step 3** In the Run field, enter **cmd** and click **OK**.

**Step 4** In the command prompt window, enter **c:** and press **Enter**.

**Step 5** Enter **cd i386** and press **Enter**.

**Step 6** Enter **expand.exe tftp.ex\_ c:\windows\system32\tftp.exe** and press **Enter**.

**Step 7** Close the command prompt window.

### To Enable Cisco Unified CM Authentication and Encryption for Cisco Unity Connection Voice Messaging Ports

**Step 1** If Cisco Unity Connection Administration is not already open, log on to Cisco Unity Connection Administration.

**Step 2** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.

**Step 3** On the Search Ports page, click the display name of the first voice messaging port for the Cisco Unified CM 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 4** On the Port Basics page, confirm that the Security Mode field is set to the applicable setting.




**Caution** The Security Mode setting for Cisco Unity Connection voice messaging ports must match the security mode setting for the Cisco Unified CM ports. Otherwise, Cisco Unified CM authentication and encryption will fail.

**Table 20 Security Mode Settings**

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port.  In addition, the media stream will not be encrypted.
Authenticated	The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text.  In addition, the media stream will not be encrypted.
Encrypted	The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted.  In addition, the media stream can be encrypted.

- Step 5** If you changed the setting, click **Save** and click **Next**.
- Step 6** Repeat [Step 4](#) and [Step 5](#) for all remaining voice messaging ports for the Cisco Unified CM phone system integration.
- Step 7** Restart the Cisco Unity Connection software.  
  
Cisco Unity Connection generates the voice messaging port device certificates and the Cisco Unity Connection root certificate.
- Step 8** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.
- Step 9** On the Search Phone Systems page, click the name of the Cisco Unified CM phone system for which you want to enable authentication and encryption of the Cisco Unity Connection voice messaging ports.
- Step 10** On the Phone System Basics page, on the Edit menu, click **Root Certificate**.
- Step 11** On the View Root Certificate page, right-click the **Right-click to Save the Certificate as a File** link, and click **Save Target As**.
- Step 12** In the Save As dialog box, browse to the location on the Cisco Unity Connection server where you want to save the Cisco Unity Connection root certificate as a file.
- Step 13** In the File Name field, confirm that the extension is .pem (rather than .htm), and click **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.

When Cisco Unity Connection is integrated with both Cisco Unified CM 4.x and Cisco Unified CM 5.x and later servers, you must copy the .pem file to the Cisco Unified CM 5.x and later servers and the .0 file to the Cisco Unified CM 4.x server. Otherwise, authentication and encryption will not function correctly.

- Step 14** In the Download Complete dialog box, click **Close**.

- Step 15** Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.



**Caution** The Cisco Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM will not let the Cisco Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Cisco Unity Connection device certificates.

- a. On the Cisco Unified CM server, in Cisco Unified CM Platform Administration, on the Security menu, click **Certificate Management > Upload Certificate/CTL**.
- b. On the Cisco IPT Platform Administration page, click **Upload Trust Certificate and CallManager - Trust**, then click **OK**.
- c. Browse to the Cisco Unity Connection root certificate that you saved in [Step 13](#).
- d. Follow the on-screen instructions.
- e. Repeat [Step 15a.](#) through [Step 15d.](#) on all remaining Cisco Unified CM servers in the cluster.
- f. In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **Go** to confirm the connection to the Cisco Unified CM servers.  
If the test is not successful, the Task Results list displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.
- g. In the Task Results window, click **Close**.

- Step 16** If prompted, restart the Cisco Unity Connection software.

- Step 17** Log off Cisco Unity Connection Administration.

## Testing the Integration

To test whether Cisco Unity Connection and the phone system are integrated correctly, do the following procedures in the order listed.

If any of the steps indicate a failure, refer to the following documentation as applicable:

- The installation guide for the phone system.
- The setup information earlier in this guide.

### To Set Up the Test Configuration

- Step 1** Set up two test extensions (Phone 1 and Phone 2) on the same phone system that Cisco Unity Connection is connected to.
- Step 2** Set Phone 1 to forward calls to the Cisco Unity Connection pilot number when calls are not answered.



**Caution** The phone system must forward calls to the Cisco Unity Connection pilot number in no fewer than four rings. Otherwise, the test may fail.

- Step 3** To create a test user for testing, in Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 4** On the Search Users page, on the User menu, click **New User**.
- Step 5** On the New User page, enter the following settings.

**Table 21** *Settings for the New User Page*

Field	Setting
User Type	<b>User with Voice Mailbox</b>
Based on Template	<the applicable user template>
Alias	<b>testuser</b>
First Name	<b>Test</b>
Last Name	<b>User</b>
Display Name	<b>Test User</b>
Extension	<the extension of Phone 1>

- Step 6** Click **Save**.
- Step 7** On the Edit User Basics page, in the Voice Name field, record a voice name for the test user.
- Step 8** In the Phone System field, confirm that the phone system selected is the phone system that Phone 1 is connected to.
- Step 9** Uncheck the **Set for Self-enrollment at Next Login** check box.
- Step 10** Click **Save**.
- Step 11** On the Edit menu, click **Message Waiting Indicators**.
- Step 12** On the Message Waiting Indicators page, click the message waiting indicator. If no message waiting indication is in the table, click **Add New**.
- Step 13** On the Edit Message Waiting Indicator page, enter the following settings.

**Table 22** *Settings for the Edit MWI Page*

Field	Setting
Enabled	Check this check box to enable MWIs for the test user.
Display Name	Accept the default or enter a different name.
Inherit User's Extension	Check this check box to enable MWIs on Phone 1.

- Step 14** Click **Save**.
- Step 15** On the Edit menu, click **Transfer Options**.
- Step 16** On the Transfer Options page, click the active option.
- Step 17** On the Edit Transfer Option page, under Transfer Action, click the **Extension** option and enter the extension of Phone 1.
- Step 18** In the Transfer Type field, click **Release to Switch**.
- Step 19** Click **Save**.

- Step 20** Minimize the Cisco Unity Connection Administration window.  
Do not close the Cisco Unity Connection Administration window because you will use it again in a later procedure.
- Step 21** On the Cisco Unity Connection desktop, double-click the **Tools Depot** icon.
- Step 22** In the left pane of the Tools Depot window, expand **Switch Integration Tools**, then double-click **Port Status Monitor**. The Port Status Monitor window appears.
- Step 23** On the Ports menu, click **Start All**, and arrange the port monitors so that you can notice which port will handle the calls that you will make.
- 

#### To Test an External Call with Release Transfer

---

- Step 1** From Phone 2, enter the access code necessary to get an outside line, then enter the number outside callers use to dial directly to Cisco Unity Connection.
- Step 2** In the Port Status Monitor, note which port handles this call.
- Step 3** When you hear the opening greeting, enter the extension for Phone 1. Hearing the opening greeting means that the port is configured correctly.
- Step 4** Confirm that Phone 1 rings and that you hear a ringback tone on Phone 2. Hearing a ringback tone means that Cisco Unity Connection correctly released the call and transferred it to Phone 1.
- Step 5** Leaving Phone 1 unanswered, confirm that the state of the port handling the call changes to “Idle.” This state means that release transfer is successful.
- Step 6** Confirm that, after the number of rings that the phone system is set to wait, the call is forwarded to Cisco Unity Connection and that you hear the greeting for the test user. Hearing the greeting means that the phone system forwarded the unanswered call and the call-forward information to Cisco Unity Connection, which correctly interpreted the information.
- Step 7** On the Port Status Monitor, note which port handles this call.
- Step 8** Leave a message for the test user and hang up Phone 2.
- Step 9** In the Port Status Monitor, confirm that the state of the port handling the call changes to “Idle.” This state means that the port was successfully released when the call ended.
- Step 10** Confirm that the MWI on Phone 1 is activated. The activated MWI means that the phone system and Cisco Unity Connection are successfully integrated for turning on MWIs.
- 

#### To Test Listening to Messages

---

- Step 1** From Phone 1, enter the internal pilot number for Cisco Unity Connection.
- Step 2** When asked for your password, enter the password for the test user. Hearing the request for your password means that the phone system sent the necessary call information to Cisco Unity Connection, which correctly interpreted the information.
- Step 3** Confirm that you hear the recorded voice name for the test user (if you did not record a voice name for the test user, you will hear the extension number for Phone 1). Hearing the voice name means that Cisco Unity Connection correctly identified the user by the extension.
- Step 4** Listen to the message.

- Step 5** After listening to the message, delete the message.
- Step 6** Confirm that the MWI on Phone 1 is deactivated. The deactivated MWI means that the phone system and Cisco Unity Connection are successfully integrated for turning off MWIs.
- Step 7** Hang up Phone 1.
- Step 8** On the Port Status Monitor, confirm that the state of the port handling the call changes to “Idle.” This state means that the port was successfully released when the call ended.

### To Set Up Supervised Transfer on Cisco Unity Connection

- Step 1** In Cisco Unity Connection Administration, on the Edit Transfer Option page for the test user, in the Transfer Type field, click **Supervise Transfer**.
- Step 2** In the Rings to Wait For field, enter **3**.
- Step 3** Click **Save**.
- Step 4** Minimize the Cisco Unity Connection Administration window.  
Do not close the Cisco Unity Connection Administration window because you will use it again in a later procedure.

### To Test Supervised Transfer

- Step 1** From Phone 2, enter the access code necessary to get an outside line, then enter the number outside callers use to dial directly to Cisco Unity Connection.
- Step 2** On the Port Status Monitor, note which port handles this call.
- Step 3** When you hear the opening greeting, enter the extension for Phone 1. Hearing the opening greeting means that the port is configured correctly.
- Step 4** Confirm that Phone 1 rings and that you do not hear a ringback tone on Phone 2. Instead, you should hear the indication your phone system uses to mean that the call is on hold (for example, music).
- Step 5** Leaving Phone 1 unanswered, confirm that the state of the port handling the call remains “Busy.” This state and hearing an indication that you are on hold mean that Cisco Unity Connection is supervising the transfer.
- Step 6** Confirm that, after three rings, you hear the greeting for the test user. Hearing the greeting means that Cisco Unity Connection successfully recalled the supervised-transfer call.
- Step 7** During the greeting, hang up Phone 2.
- Step 8** On the Port Status Monitor, confirm that the state of the port handling the call changes to “Idle.” This state means that the port was successfully released when the call ended.
- Step 9** Exit the Port Status Monitor.

### To Delete the Test User

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then click **Users**.
- Step 2** On the Search Users page, check the check box to the left of the test user.

**Step 3** Click **Delete Selected**.

---

If Cisco Unity Connection is set up for Cisco Unified CM authentication or encryption, do the following procedure.

**To Test Cisco Unified CM Authentication and Encryption**

---

**Step 1** From Phone 1, dial the internal pilot number for Cisco Unity Connection.

**Step 2** Confirm that the authentication icon and/or the encryption icon appear on the LCD of the phone.

**Step 3** Hang up Phone 1.

---

## (Multiple Integrations Only) Adding New User Templates

When you create the first phone system integration, this phone system is automatically selected in the default user template. The users that you add after creating this phone system integration will be assigned to this phone system by default.

However, for each additional phone system integration that you create, you must add the applicable new user templates that will assign users to the new phone system. You must add the new templates before you add new users who will be assigned to the new phone system.

For details on adding new user templates, refer to the “Adding, Changing, or Deleting an Account Template” chapter in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* 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).

For details on selecting a user template when adding a new user, refer to the applicable chapter for adding user accounts in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* 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).

## Changing the Number of Voice Messaging Ports

To change the number of voice messaging ports in Cisco Unified CM and in Cisco Unity Connection for an existing integration, do the following procedures.

**To Change the Number of Voice Mail Ports in Cisco Unified CM Administration**

---

**Step 1** On the Cisco Unified CM server, use the Cisco Voice Mail Port Wizard to change the number of voice mail ports. Refer to the following:

- To add voice mail ports in Cisco Unified CM Administration by using the Cisco Voice Mail Port Wizard, see the “[To Add Voice Mail Ports to Cisco Unified CM](#)” procedure on page 9.
  - To remove voice mail ports in Cisco Unified CM Administration by using the Cisco Voice Mail Port Wizard, refer to Cisco Unified CM Administration Help.
-

If you are adding voice messaging ports, do the [“To Add Voice Messaging Ports in Cisco Unity Connection Administration” procedure on page 30](#).

If you are deleting voice messaging ports, do the [“To Delete Voice Messaging Ports in Cisco Unity Connection Administration” procedure on page 31](#).

### To Add Voice Messaging Ports in Cisco Unity Connection Administration

- 
- Step 1** If the Cisco Unity Connection license does not enable the additional voice messaging ports you added, see your sales representative to request the applicable license.
  - Step 2** When you have the license, log on to Cisco Unity Connection Administration.
  - Step 3** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
  - Step 4** On the License page, on the License menu, click **Add New License**.
  - Step 5** On the Add New License page, click **Browse**.
  - Step 6** In the Choose File dialog box, browse to the license file and click **Open**.
  - Step 7** On the Add New License page, click **Add**.
  - Step 8** On the Licenses page, check the check box for the license file that you added in [Step 7](#) and click **Install Selected**.
  - Step 9** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.
  - Step 10** On the Search Ports page, under Port Search Results, click **Add New**.
  - Step 11** On the New Port page, enter the applicable settings and click **Save**.




---

**Caution** Make sure that there are an appropriate number of ports set to answer calls and an appropriate number of ports set to dial out. Otherwise, the integration will not function correctly. For details, see to the “Planning How the Voice Messaging Ports Will be Used by Cisco Unity Connection” section.

---

- Step 12** If prompted to restart Cisco Unity Connection, in the Windows task bar, right-click the **Cisco Unity Connection** icon and click **Restart > Voice Processing Server Role**.
- Step 13** When prompted to confirm stopping the Voice Processing server role, click **Yes**.
- Step 14** If you are not using Cisco Unified CM authentication and encryption, skip to [Step 22](#).  
If you are using Cisco Unified CM authentication and encryption, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Phone System**.




---

**Caution** Confirm that you have set up the TFTP server on the Edit Servers page for the port group that the voice messaging ports belong to. Otherwise, the integration will not function correctly with Cisco Unified CM authentication and encryption.

---

- Step 15** On the Search Phone Systems page, click the name of the Cisco Unified CM phone system for which you want to enable authentication and encryption of the Cisco Unity Connection voice messaging ports.
- Step 16** On the Phone System Basics page, on the Edit menu, click **Root Certificate**.
- Step 17** On the View Root Certificate page, right-click the **Right-click to Save the Certificate as a File** link, and click **Save Target As**.

**Step 18** In the Save As dialog box, browse to the location on the Cisco Unity Connection server where you want to save the Cisco Unity Connection root certificate as a file.

**Step 19** In the File Name field, confirm that the extension is .pem (rather than .htm), and click **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.

When Cisco Unity Connection is integrated with both Cisco Unified CM 4.x and Cisco Unified CM 5.x or later servers, you must copy the .pem file to the Cisco Unified CM 5.x or later servers and the .0 file to the Cisco Unified CM 4.x server. Otherwise, authentication and encryption will not function correctly.

**Step 20** In the Download Complete dialog box, click **Close**.

**Step 21** Upload the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.



**Caution** The Cisco Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM will not let the Cisco Unity Connection voice messaging ports register until the Cisco Unified CM system clock has passed the time stamp in the Cisco Unity Connection device certificates.

- a. On the Cisco Unified CM server, in Cisco Unified CM Platform Administration, on the Security menu, click **Certificate Management > Upload Certificate/CTL**.
- b. On the Cisco IPT Platform Administration page, click **Upload Trust Certificate and CallManager - Trust**, then click **OK**.
- c. Browse to the Cisco Unity Connection root certificate that you saved in [Step 19](#).
- d. Follow the on-screen instructions.
- e. Repeat [Step 21a.](#) through [Step 21d.](#) on all remaining Cisco Unified CM servers in the cluster.
- f. In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **Go** to confirm the connection to the Cisco Unified CM servers.  
If the test is not successful, the Task Results list displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.
- g. In the Task Results window, click **Close**.

**Step 22** If prompted, restart the Cisco Unity Connection software.

**Step 23** Log off Cisco Unity Connection Administration.

---

### To Delete Voice Messaging Ports in Cisco Unity Connection Administration

**Step 1** Log on to the Cisco Unity Connection Administration.

**Step 2** Go to the **Telephony Integrations > Port** page.

**Step 3** Under Port Search Results, check the check boxes next to the voice messaging ports that you want to delete.

- Step 4** Click **Delete Selected**.
- Step 5** For the remaining voice messaging ports in the port group, change the settings as necessary so that there are an appropriate number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out.
- Step 6** In the Windows task bar, right-click the **Cisco Unity Connection** icon and click **Restart > Voice Processing Server Role**.
- Step 7** When prompted to confirm stopping the Voice Processing server role, click **Yes**.
- Step 8** In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Check Telephony Configuration** and click **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 9** In the Task Execution Results window, click **Close**.
- Step 10** Log off the Cisco Unity Connection Administration.

## Adding a Cisco Unified Communications Manager Express Server to a Cisco Unified Communications Manager Phone System Integration

Cisco Unity Connection can integrate a Cisco Unified CM phone system integration that has a port group of Cisco Unified CM servers and a port group of a Cisco Unified CM Express server. This configuration is typically used to ensure call processing functionality at a branch office when the WAN link is down.

There are, however, the following considerations:

- The version of Cisco Unified CM Express and the version of the Cisco Unity-CM TSP must be a supported combination in the *SCCP 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).
- The Cisco Unified CM phone system integration is typically already created before adding the Cisco Unified CM Express server.

To add a Cisco Unified CM Express server to a Cisco Unified CM phone system integration, do the following procedure.

### To Add a Cisco Unified CM Express Server to a Cisco Unified CM Phone System Integration

- Step 1** Log on to Cisco Unity Connection Administration.
- Step 2** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port Group**.
- Step 3** On the Search Port Groups page, click the name of the port group for the Cisco Unified CM servers.
- Step 4** On the Port Group Basics page, on the Edit menu, click **Servers**.
- Step 5** On the Edit Servers page, under Cisco Unified CallManager Servers, click **Add**.
- Step 6** In the row for Cisco Unified CM servers, enter the following settings.

**Table 23**      **Settings for the Cisco Unified CM Express Server**

Field	Setting
IP Address or Host Name	Enter the IP address (or host name) of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group.
Port	Enter the TCP port of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group. We recommend that you use the default setting.
Server Type	Click <b>Cisco CallManager Express</b> .



**Note**      You can click **Ping** to verify the IP address of the Cisco Unified CM Express server.

- Step 7**      Click **Save**.
- Step 8**      On the Edit menu, click **Advanced Settings**.
- Step 9**      On the Edit Advanced Settings page, in the Delay Before Opening Greeting field, enter **1000** and click **Save**.
- Step 10**     In the Windows task bar, right-click the **Cisco Unity Connection** icon and click **Restart > Voice Processing Server Role**.
- Step 11**     When prompted to confirm stopping the Voice Processing server role, click **Yes**.
- Step 12**     In Cisco Unity Connection Administration, in the Related Links drop-down list, click **Test Port Group** and click **Go** to confirm the Cisco Unified CM port group settings.
- Step 13**     When prompted that the test will terminate call in progress, click **OK**.  
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 14**     In the Task Execution Results window, click **Close**.
- Step 15**     Log off Cisco Unity Connection Administration.

## Appendix: Cisco Unified Communications Manager Authentication and Encryption of Cisco Unity Connection Voice Messaging Ports

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Cisco Unity Connection and Cisco Unified CM. Possible threats include:

- Man-in-the-middle attacks (a process in which an attacker observes and modifies the information flow between Cisco Unified CM and the Cisco Unity Connection voice messaging ports)
- Network traffic sniffing (a process in which an attacker uses software to capture phone conversations and signaling information that flow between Cisco Unified CM, the Cisco Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between the Cisco Unity Connection voice messaging ports and Cisco Unified CM
- Modification of the media stream between the Cisco Unity Connection voice messaging ports and the endpoint (for example, a phone or gateway)
- Identity theft of the Cisco Unity Connection voice messaging port (a process in which a non-Cisco Unity Connection device presents itself to Cisco Unified CM as a Cisco Unity Connection voice messaging port)
- Identity theft of the Cisco Unified CM server (a process in which a non-Cisco Unified CM server presents itself to Cisco Unity Connection voice messaging ports as a Cisco Unified CM server)

# Cisco Unified Communications Manager Security Features

Cisco Unified CM can secure the connection with Cisco Unity Connection against these threats. The Cisco Unified CM security features that Cisco Unity Connection can take advantage of are described in [Table 24](#).

**Table 24** *Cisco Unified CM Security Features That Are Used by Cisco Unity Connection*

Security Feature	Description
Signaling authentication	<p>The process that uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file.</p> <p><b>Impact on Threats:</b> This feature protects against:</p> <ul style="list-style-type: none"> <li>• Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity Connection voice messaging ports.</li> <li>• Modification of the call signalling.</li> <li>• Identity theft of the Cisco Unity Connection voice messaging port.</li> <li>• Identity theft of the Cisco Unified CM server.</li> </ul>
Device authentication	<p>The process that validates the identity of the device and ensures that the entity is what it claims to be. This process occurs between Cisco Unified CM and Cisco Unity Connection voice messaging ports when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file.</p> <p><b>Impact on Threats:</b> This feature protects against:</p> <ul style="list-style-type: none"> <li>• Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity Connection voice messaging ports.</li> <li>• Modification of the media stream.</li> <li>• Identity theft of the Cisco Unity Connection voice messaging port.</li> <li>• Identity theft of the Cisco Unified CM server.</li> </ul>

**Table 24** Cisco Unified CM Security Features That Are Used by Cisco Unity Connection

Security Feature	Description
Signaling encryption	<p>The process that uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP signaling messages that are sent between the Cisco Unity Connection voice messaging ports and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access.</p> <p><b>Impact on Threats:</b> This feature protects against:</p> <ul style="list-style-type: none"> <li>• Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and the Cisco Unity Connection voice messaging ports.</li> <li>• Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and the Cisco Unity Connection voice messaging ports.</li> </ul>
Media encryption	<p>The process whereby the confidentiality of the media occurs through the use of cryptographic procedures. This process uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711, and ensures that only the intended recipient can interpret the media streams between Cisco Unity Connection voice messaging ports and the endpoint (for example, a phone or gateway). Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to Cisco Unity Connection and the endpoint, and securing the delivery of the keys while the keys are in transport. Cisco Unity Connection and the endpoint use the keys to encrypt and decrypt the media stream.</p> <p><b>Impact on Threats:</b> This feature protects against:</p> <ul style="list-style-type: none"> <li>• Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and the Cisco Unity Connection voice messaging ports.</li> <li>• Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, the Cisco Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM.</li> </ul>

Authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur.

**Note**

Cisco Unified CM authentication and encryption protects only calls to Cisco Unity Connection. Messages recorded on the message store are not protected by the Cisco Unified CM authentication and encryption features.

# Functional Overview

The security features (authentication and encryption) between Cisco Unity Connection and Cisco Unified CM require the following:

- A Cisco Unified CM CTL file that lists all Cisco Unified CM servers that are entered in Cisco Unity Connection Administration for secure clusters.
- A Cisco Unity Connection server root certificate for each Cisco Unity Connection server that uses authentication and/or encryption. A root certificate is valid for 20 years from the time it was created.
- Cisco Unity Connection voice messaging port device certificates that are rooted in the Cisco Unity Connection server root certificate and that the voice messaging ports present when registering with the Cisco Unified CM server.

The process of authentication and encryption of Cisco Unity Connection voice messaging ports is as follows:

1. Each Cisco Unity Connection voice messaging port connects to the TFTP server, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Cisco Unity Connection voice messaging port establishes a network connection to the Cisco Unified CM TLS port. By default, the TLS port is 2443, though the port number is configurable.
3. Each Cisco Unity Connection voice messaging port establishes a TLS connection to the Cisco Unified CM server, at which time the device certificate is verified and the voice messaging port is authenticated.
4. Each Cisco Unity Connection voice messaging port registers with the Cisco Unified CM server, specifying whether the voice messaging port will also use media encryption.

## Behavior for Calls


When a call is made between Cisco Unity Connection and Cisco Unified CM, the call-signaling messages and the media stream are handled in the following manner:

- If both end points are set for encrypted mode, the call-signaling messages and the media stream are encrypted.
- If one end point is set for authenticated mode and the other end point is set for encrypted mode, the call-signaling messages are authenticated. But neither the call-signaling messages nor the media stream are encrypted.
- If one end point is set for non-secure mode and the other end point is set for encrypted mode, neither the call-signaling messages nor the media stream are encrypted.

# Security Mode Settings in Cisco Unity Connection

The Security Mode settings in Cisco Unity Connection Administration determine how the ports handle call-signaling messages and whether encryption of the media stream is possible. Table 25 describes the effect of the Security Mode settings on the Telephony Integrations > Port > Port Basics page for each port.

**Table 25 Security Mode Settings for Voice Messaging Ports**

Setting	Effect
Non-secure	<p>The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port.</p> <p>In addition, the media stream cannot be encrypted.</p>
Authenticated	<p>The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text.</p> <p>In addition, the media stream will not be encrypted.</p>
Encrypted	<p>The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted.</p> <p>In addition, the media stream can be encrypted.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> <b>Caution</b> Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted.</p> </div>

### Disabling and Re-Enabling Security

The authentication and encryption features between Cisco Unity Connection and Cisco Unified CM can be enabled and disabled by changing the Security Mode for all Cisco Unified CM clusters to Non-Secure, and by changing the applicable settings in the Cisco Unified CM Administration.

Authentication and encryption can be re-enabled by changing the Security Mode to Authenticated or Encrypted.



**Note**

After disabling or re-enabling authentication and encryption, it is not necessary to export the Cisco Unity Connection server root certificate and copy it to all Cisco Unified CM servers.

### Multiple Clusters Can Have Multiple Settings

When Cisco Unity Connection has multiple Cisco Unified CM phone system integrations, each Cisco Unified CM phone system integration can have different Security Mode settings. For example, one Cisco Unified CM phone system integration can be set to Encrypted, and a second Cisco Unified CM phone system integration can be set to Non-Secure.

### Settings for Individual Voice Messaging Ports

For troubleshooting purposes, authentication and encryption for Cisco Unity Connection voice messaging ports can be individually enabled and disabled. At all other times, we recommend that the Security Mode setting for all individual voice messaging ports in a Cisco Unified CM port group be the same.

## Appendix: Documentation and Technical Assistance

### Documentation Conventions

The *Cisco Unified Communications Manager 6.x SCCP Integration Guide for Cisco Unity Connection 1.2* uses the following conventions.

**Table 26** *Cisco Unified Communications Manager 6.x SCCP Integration Guide for Cisco Unity Connection 1.2 Conventions*

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none"> <li>• Key and button names. (Example: Click <b>OK</b>.)</li> <li>• Information that you enter. (Example: Enter <b>Administrator</b> in the User Name box.)</li> </ul>
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter <b>ping &lt;IP address&gt;</b> .)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press <b>Ctrl-Alt-Delete</b> .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, click <b>Programs &gt; Cisco Unified Serviceability &gt; Real-Time Monitoring Tool</b> .)  In the navigation bar of the Cisco Unity Connection Administration. (Example: In the Cisco Unity Connection Administration, expand <b>System Settings &gt; Advanced</b> .)

The *Cisco Unified Communications Manager 6.x SCCP Integration Guide for Cisco Unity Connection 1.2* also uses the following conventions:



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Cisco Unity Connection and is available at [http://www.cisco.com/en/US/products/ps6509/products\\_documentation\\_roadmaps\\_list.html](http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html).

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.