



Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection

Release 10.x

Revised November, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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.

Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 10.x
© 2014 Cisco Systems, Inc. All rights reserved.



Preface vii

Audience and Use vii

Documentation Conventions vii

Cisco Unity Connection Documentation viii

Obtaining Documentation and Submitting a Service Request viii

Cisco Product Security Overview viii

CHAPTER 1

Introduction 1-1

Integration Description 1-1

Call Information 1-1

Integration Functionality 1-2

Integrations with Multiple Phone Systems 1-3

CHAPTER 2

Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection 2-1

Introduction: Issues to Consider When Planning Port Setup 2-1

Determining How Many Voice Messaging Ports to Install 2-2

Determining How Many Voice Messaging Ports Will Answer Calls 2-3

Determining How Many Voice Messaging Ports Will Only Dial Out, and Not Answer Calls 2-3

Considerations for a Cisco Unity Connection Cluster 2-3

 When Both Cisco Unity Connection Servers Are Functioning Normally 2-3

 When Only One Cisco Unity Connection Server Is Functioning 2-4

CHAPTER 3

Setting Up a Cisco Unified Communications Manager 5.x SIP Trunk Integration with Cisco Unity Connection 3-1

Integration Tasks 3-1

Requirements 3-2

Centralized Voice Messaging 3-3

Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection 3-3

 For Cisco Unity Connection Without a Unity Connection Cluster 3-3

 For Cisco Unity Connection with a Unity Connection Cluster Configured 3-9

Creating a New Integration with Cisco Unified Communications Manager 3-18

CHAPTER 4

Setting Up a Cisco Unified Communications Manager 6.x SIP Trunk Integration with Cisco Unity Connection 4-1

Integration Tasks 4-1

Requirements 4-2

Centralized Voice Messaging 4-3

Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection 4-3

For Cisco Unity Connection Without a Unity Connection Cluster 4-3

For Cisco Unity Connection with a Unity Connection Cluster Configured 4-9

Creating a New Integration with Cisco Unified Communications Manager 4-18

CHAPTER 5

Setting Up a Cisco Unified Communications Manager 7.x SIP Trunk Integration with Cisco Unity Connection 5-1

Integration Tasks 5-1

Requirements 5-2

Centralized Voice Messaging 5-3

Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection 5-3

For Cisco Unity Connection Without a Unity Connection Cluster 5-3

For Cisco Unity Connection with a Unity Connection Cluster Configured 5-9

Creating a New Integration with Cisco Unified Communications Manager 5-18

CHAPTER 6

Setting Up a Cisco Unified Communications Manager 10.x SIP Trunk Integration with Cisco Unity Connection 6-1

Integration Tasks 6-1

Requirements 6-2

Centralized Voice Messaging 6-3

Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection 6-3

For Cisco Unity Connection Without a Unity Connection Cluster 6-3

For Cisco Unity Connection with a Unity Connection Cluster Configured 6-10

Creating a New Integration with Cisco Unified Communications Manager 6-19

CHAPTER 7	Testing the Integration	7-1
CHAPTER 8	Adding New User Templates for Multiple Integrations	8-1
APPENDIX A	Adding Cisco Unified Communications Manager Express to a Cisco Unified Communications Manager Integration	A-1
INDEX		



Preface

This Preface contains the following sections:

- [Audience and Use, page 7](#)
- [Documentation Conventions, page 7](#)
- [Cisco Unity Connection Documentation, page 8](#)
- [Obtaining Documentation and Submitting a Service Request, page 8](#)
- [Cisco Product Security Overview, page 8](#)

Audience and Use

This document provides instructions for setting up an integration between Cisco Unity Connection and supported versions of Cisco Unified Communications Manager. For a list of supported versions of Cisco Unified CM that are qualified to integrate with Cisco Unity Connection through a SIP trunk, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.

Documentation Conventions

The *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 10.x* uses the following conventions.

Table 1 *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 10.x Conventions*

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none">• Key and button names. (Example: Select OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter ping <IP address> .)

Table 1 *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 10.x Conventions (continued)*

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press Ctrl-Alt-Delete .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make on menus. (Example: On the Windows Start menu, select Programs > Cisco Unified Serviceability > Real-Time Monitoring Tool .) In the navigation bar of the Cisco Unity Connection Administration. (Example: In the Cisco Unity Connection Administration, expand System Settings > Advanced .)

The *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 10.x* also uses the following conventions:

Cisco Unity Connection Documentation

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.

Documentation References to Cisco Business Edition

In Cisco Unity Connection 10.x documentation set, references to Cisco Business Edition apply on Business Edition 6000 and 7000.

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.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors

and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at http://www.access.gpo.gov/bis/ear/ear_data.html.





Introduction

See the following sections in this chapter:

- [Integration Description, page 1-1](#)
- [Call Information, page 1-1](#)
- [Integration Functionality, page 1-2](#)
- [Integrations with Multiple Phone Systems, page 1-3](#)

Integration Description

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

For a list of supported versions of Cisco Unified CM that are qualified to integrate with Cisco Unity Connection through a SIP trunk, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.

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

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 without this information, Cisco Unity Connection answers with the opening greeting.

Integration Functionality

The Cisco Unified CM SIP trunk 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 a 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, see the “Integrating Voice Mail with Cisco Unified SRST” chapter of the applicable *Cisco Unified SRST System Administrator Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html.

Impact of Non-Delivery of RDNIS on Voicemail 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 voicemail 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 voicemail 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 two or more phone systems at one time. For information on the maximum supported combinations and instructions for integrating Cisco Unity Connection with multiple phone systems, see the *Multiple Phone System Integration Guide for Cisco Unity Connection Release 10.x* at 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

See the following sections in this chapter:

- [Introduction: Issues to Consider When Planning Port Setup, page 2-1](#)
- [Determining How Many Voice Messaging Ports to Install, page 2-2](#)
- [Determining How Many Voice Messaging Ports Will Answer Calls, page 2-3](#)
- [Determining How Many Voice Messaging Ports Will Only Dial Out, and Not Answer Calls, page 2-3](#)
- [Considerations for a Cisco Unity Connection Cluster, page 2-3](#)


Introduction: Issues to Consider When Planning Port Setup

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.
For a Cisco Unity Connection cluster, each Cisco Unity Connection server must have enough ports to handle all voice messaging traffic in case the other server stops functioning.
- 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 2-1 Settings for the Voice Messaging Ports

Field	Considerations
Enabled	Check this check box.
Server	<p>(When a Cisco Unity Connection cluster is configured) Select the name of the Cisco Unity Connection server that you want to handle this port.</p> <p>Assign an equal number of answering and dial-out voice messaging ports to the Cisco Unity Connection servers so that they equally share the voice messaging traffic.</p>
Answer Calls	<p>Check this check box.</p> <p> Caution All voice messaging ports connecting to the Cisco Unified CM server must have the Answer Calls box checked. Otherwise, calls to Cisco Unity Connection may not be answered.</p>
Perform Message Notification	Check this check box to designate the port for notifying subscribers of messages.
Send MWI Requests	Check this check box to designate the port for turning MWIs on and off.
Allow TRAP Connections	Check this check box so that users can use the phone as a recording and playback device in Cisco Unity Connection web applications.

Determining How Many 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.
- Whether a Cisco Unity Connection cluster is configured. For considerations, see the [“Considerations for a Cisco Unity Connection Cluster”](#) section on page 2-3.

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.

Determining How Many Voice Messaging Ports 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.

If your system is configured for a Cisco Unity Connection cluster, see the [“Considerations for a Cisco Unity Connection Cluster” section on page 2-3](#).

Determining How Many Voice Messaging Ports 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 email 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.

If your system is configured for a Cisco Unity Connection cluster, see the [“Considerations for a Cisco Unity Connection Cluster” section on page 2-3](#).



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.

Considerations for a Cisco Unity Connection Cluster

If your system is configured for a Cisco Unity Connection cluster, consider how the voice messaging ports will be used in different scenarios.

When Both Cisco Unity Connection Servers Are Functioning Normally

- A hunt group is configured to send incoming calls first to the subscriber server, then to the publisher server if no answering ports are available on the subscriber server.

- Both Cisco Unity Connection servers are active and handle voice messaging traffic for the system.
- In Cisco Unity Connection Administration, the voice messaging ports are configured so that an equal number of voice messaging ports are assigned to each Cisco Unity Connection server. This guide directs you to assign the voice messaging ports to their specific server at the applicable time.
- The number of voice messaging ports that are assigned to one Cisco Unity Connection server must be sufficient to handle all of the voice messaging traffic for the system (answering calls and dialing out) when the other Cisco Unity Connection server stops functioning.

If both Cisco Unity Connection servers must be functioning to handle the voice messaging traffic, the system will not have sufficient capacity when one of the servers stops functioning.

- Each Cisco Unity Connection server is assigned half the total number of voice messaging ports.
If all the voice messaging ports are assigned to one Cisco Unity Connection server, the other Cisco Unity Connection server will not be able to answer calls or to dial out.
- Each Cisco Unity Connection server must have voice messaging ports that will answer calls and that can dial out (for example, to set MWIs).

When Only One Cisco Unity Connection Server Is Functioning

- The hunt group on the phone system sends all calls to the functioning Cisco Unity Connection server.
- The functioning Cisco Unity Connection server receives all voice messaging traffic for the system.
- The number of voice messaging ports that are assigned to the functioning Cisco Unity Connection server must be sufficient to handle all of the voice messaging traffic for the system (answering calls and dialing out).
- The functioning Cisco Unity Connection server must have voice messaging ports that will answer calls and that can dial out (for example, to set MWIs).

If the functioning Cisco Unity Connection server does not have voice messaging ports for answering calls, the system will not be able to answer incoming calls. Similarly, if the functioning Cisco Unity Connection server does not have voice messaging ports for dialing out, the system will not be able to dial out (for example, to set MWIs).



Setting Up a Cisco Unified Communications Manager 5.x SIP Trunk Integration with Cisco Unity Connection

For detailed instructions for setting up a Cisco Unified Communications Manager 5.x SIP trunk integration with Cisco Unity Connection, see the following sections in this chapter:

- [Integration Tasks, page 3-1](#)
- [Requirements, page 3-2](#)
- [“Centralized Voice Messaging” section on page 3-3](#)
- [Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection, page 3-3](#)
- [Creating a New Integration with Cisco Unified Communications Manager, page 3-18](#)

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



Note

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

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

Integration Tasks

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

1. Review the system and equipment requirements to confirm that all phone system and Cisco Unity Connection server requirements have been met. See the [“Requirements” section on page 3-2](#).
2. Plan how the voice messaging ports will be used by Cisco Unity Connection. See [Chapter 2, “Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection.”](#)

3. Program Cisco Unified CM. See the “Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection” section on page 3-3.
4. Create the integration. See the “Creating a New Integration with Cisco Unified Communications Manager” section on page 3-18.



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

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

Requirements

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

Phone System

- Cisco Unified CM 5.x.
For details on compatible versions of Cisco Unified CM, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- For the Cisco Unified CM extensions, one of the following configurations:
 - (Best practice) Only SIP phones that support DTMF relay as described in RFC-2833.
 - Both SCCP phones and SIP phones.
Note that older SCCP phone models may require a Media Termination Point (MTP) to function correctly.
- A LAN connection in each location where you will plug the applicable phone into the network.
- For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Cisco Unified CM cluster without having to dial a trunk access code or prefix.

Cisco Unity Connection Server

- The applicable version of Cisco Unity Connection. For details on compatible versions of Cisco Unity Connection, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- 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.
- A license that enables the applicable number of voice messaging ports.

Centralized Voice Messaging

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

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

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

- **Cisco Unity Connection without a Unity Connection cluster**—Do the procedures in the “For Cisco Unity Connection Without a Unity Connection Cluster” section on page 3-3.
- **Cisco Unity Connection with a Unity Connection cluster configured**—Do the procedures in the “For Cisco Unity Connection with a Unity Connection Cluster Configured” section on page 3-9.

For Cisco Unity Connection Without a Unity Connection Cluster

Do the following procedures in the order given.



Note

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

To Create the SIP Trunk Security Profile

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

Table 3-1 Settings for the SIP Trunk Security Profile Configuration Page

Field	Setting
Name	Enter Unity Connection SIP Trunk Security Profile or another name.
Description	Enter SIP trunk security profile for Cisco Unity Connection or another description.

Table 3-1 Settings for the SIP Trunk Security Profile Configuration Page (continued)

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

Step 4 Select **Save**.

To Create the SIP Profile

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

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

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

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

Table 3-2 Settings for the SIP Profile Configuration Page

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

Step 5 Select **Save**.

To Create the SIP Trunk

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

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

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

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

Step 5 Under Device Information, enter the following settings.

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

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk or another name.
Description	Enter SIP trunk for Cisco Unity Connection or another description.

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

Table 3-4 Settings for Inbound Calls on the Trunk Configuration Page

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

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

Step 8 Under SIP Information, enter the following settings.

Table 3-5 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the Cisco Unity Connection SIP port to which Cisco Unified CM will connect.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “To Create the SIP Trunk Security Profile” procedure on page 3-3 . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.

Table 3-5 Settings for SIP Information on the Trunk Configuration Page (continued)

Field	Setting
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile” procedure on page 3-4 . For example, select “Cisco Unity Connection SIP Profile.”

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

Step 10 Select **Save**.

To Create a Route Pattern

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

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

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

Table 3-6 Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the SIP trunk that you created in the “To Create the SIP Trunk” procedure on page 3-5 . For example, select “Unity_Connection_SIP_Trunk.”

Step 4 Select **Save**.

To Create the Voice Mail Pilot

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

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

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

Table 3-7 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern” procedure on page 3-6 .
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.

Table 3-7 Settings for the Voice Mail Pilot Configuration Page (continued)

Field	Setting
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

To Set Up the Voice Mail Profile

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

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

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

Table 3-8 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot” procedure on page 3-6 .
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

To Set Up the Voice Mail Server Service Parameters

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

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

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

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 3-18.

(Optional) To Set Up SIP Digest Authentication

- Step 1** On the System menu, select **Security Profile > SIP Trunk Security Profile**.
- Step 2** On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile”](#) procedure on page 3-3.
- Step 3** On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.
- Step 4** Select **Save**.

(Optional) To Create the Application User

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

Table 3-9 Settings for the Application User Configuration Page

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.

Table 3-9 Settings for the Application User Configuration Page (continued)

Field	Setting
Presence Group	<p>Used with the Presence feature, the application user (for example, IPMASysUser) serves as the watcher because it requests status about the presence entity.</p> <p>If you want the application user to receive the status of the presence entity, make sure that the Application User Presence group is allowed to view the status of the Presence group that is applied to the directory number, as indicated in the Presence Group Configuration window.</p>
Accept Presence Subscription	Leave this check box unchecked.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Header Replacement	Leave this check box unchecked.
Available Devices	<p>This list box displays the devices that are available for association with this application user.</p> <p>To associate a device with this application user, select the device and select the Down arrow below this list box.</p> <p>If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices:</p> <ul style="list-style-type: none"> • Find More Phones—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search. • Find More Route Points—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.
Groups	This list box appears after an application user has been added. The list box displays the groups to which the application user belongs.
Roles	This list box appears after an application user has been added. The list box displays the roles that are assigned to the application user.

Step 4 Select **Save**.

For Cisco Unity Connection with a Unity Connection Cluster Configured

Do the following procedures in the order given.

**Note**

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

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

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

Table 3-10 Settings for the SIP Trunk Security Profile Configuration Page

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

Step 4 Select **Save**.

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

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

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

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

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

Table 3-11 Settings for the SIP Profile Configuration Page

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

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

Step 6 Select **Save**.

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

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

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

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

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

Step 5 Under Device Information, enter the following settings.

Table 3-12 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_1 or another name.
Description	Enter SIP trunk 1 for Cisco Unity Connection or another description.

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

Table 3-13 Settings for Inbound Calls on the Trunk Configuration Page

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

- Step 7** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.
- Step 8** Under SIP Information, enter the following settings.

Table 3-14 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the publisher Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster)” procedure on page 3-10 . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile (for a Cisco Unity Connection Cluster)” procedure on page 3-11 . For example, select “Cisco Unity Connection SIP Profile.”

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

Table 3-15 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_2 or another name.
Description	Enter SIP trunk 2 for Cisco Unity Connection or another description.

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

Table 3-16 Settings for Inbound Calls on the Trunk Configuration Page

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

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

Step 17 Under SIP Information, enter the following settings.

Table 3-17 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the subscriber Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster)” procedure on page 3-10 . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile (for a Cisco Unity Connection Cluster)” procedure on page 3-11 . For example, select “Cisco Unity Connection SIP Profile.”

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

Step 19 Select **Save**.

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

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

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

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

Table 3-18 Settings for the Route Group Configuration Page

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

Step 4 Confirm that both SIP trunks appear in the Available Devices field. Otherwise, select **Find**.

Step 5 Select **Add to Route Group**.

Step 6 Under Current Route Group Members, confirm that the SIP trunk that connects to the subscriber Cisco Unity Connection server appears first in the list.

You can select the up or down arrows to change the order of the SIP trunks.

Step 7 Select **Save**.

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

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

Table 3-19 Settings for the Route List Configuration Page

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

- Step 4** Select **Save**.
- Step 5** Confirm that the **Enable This Route List** check box is checked.
- Step 6** Under Route List Member Information, select **Add Route Group**.
- Step 7** On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the [“To Create a Route Group \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 3-13 and select **Save**.
- Step 8** When prompted that the route list settings will be saved, select **OK**.
- Step 9** On the Route List Configuration page, select **Reset**.
- Step 10** When prompted to confirm resetting the route list, select **Reset**.
- Step 11** Select **Close**.
-

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

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

Table 3-20 Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the route list that you created in the “To Create a Route List (for a Cisco Unity Connection Cluster)” procedure on page 3-14. For example, select “SIP_Trunk_Route_List.”

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

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

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

Table 3-21 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern (for a Cisco Unity Connection Cluster)” procedure on page 3-14.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

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

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

- Step 1** On the Voice Mail menu, select **Voice Mail > Voice Mail Profile**.
- Step 2** On the Find and List Voice Mail Profiles page, select **Add New**.
- Step 3** On the Voice Mail Profile Configuration page, enter the following voice mail profile settings.

Table 3-22 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot (for a Cisco Unity Connection Cluster)” procedure on page 3-15.

Table 3-22 Settings for the Voice Mail Profile Configuration Page (continued)

Field	Setting
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 3-18.

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

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

Step 2 On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 3-10.

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

Step 4 Select **Save**.

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

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

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

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

Table 3-23 Settings for the Application User Configuration Page

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

Step 4 Select **Save**.


Creating a New Integration with Cisco Unified Communications Manager

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

To Create an Integration

- Step 1** Sign in to Cisco Unity Connection Administration.
- Step 2** If you will use Cisco Unified CM authentication and encryption, do the following substeps. Otherwise, skip to [Step 3](#).
- In Cisco Unity Connection Administration, expand **Telephony Integrations**, expand **Security**, then select **SIP Certificate**.
 - On the SIP Certificates page, select **Add New**.
 - On the New SIP Certificate page, enter the following settings for the SIP certificate and select **Save**.

Table 3-24 Settings for the New SIP Certificate Page

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

- Step 3** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.
- Step 4** On the Search Phone Systems page, under Display Name, select the name of the default phone system.
- Step 5** On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.
- Step 6** If you want to use this phone system as the default for TRaP connections so that administrators and users without voicemail boxes can record and playback through the phone in Cisco Unity Connection web applications, check the **Default TRAP Switch** check box. If you want to use another phone system as the default for TRaP connections, uncheck this check box.
- Step 7** Select **Save**.
- Step 8** On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.
- Step 9** On the New Port Group page, enter the applicable settings and select **Save**.

Table 3-25 Settings for the New Port Group Page

Field	Setting
Phone System	Select the name of the phone system that you entered in Step 5 .
Create From	Select Port Group Template and select SIP in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Authenticate with SIP Server	Check this check box if you want Cisco Unity Connection to authenticate with the Cisco Unified CM server.
Authentication User Name	Enter the name that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Authentication Password	Enter the password that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users will use to contact Cisco Unity Connection and that Cisco Unity Connection will use to register with the Cisco Unified CM server.
SIP Security Profile	Select the SIP security profile that Cisco Unity Connection will use.
SIP Certificate	<i>(Only when a secure TLS port is used)</i> Confirm that the applicable SIP certificate is selected.
Security Mode	<p><i>(Only when a secure TLS port is used)</i> Select the applicable security mode:</p> <ul style="list-style-type: none"> • Authenticated—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an secure TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. • Encrypted—The integrity and privacy of call-signaling messages will be ensured on this port because they will be connected to Cisco Unified CM through an secure TLS port, and the call-signaling messages will be encrypted. <p>The Security Mode setting on the Cisco Unity Connection server must match the Device Security Mode setting on the Cisco Unified CM server.</p>
Secure RTP	<i>(Only when a secure TLS port is used)</i> Check this check box so that the media stream (RTP) is encrypted. Uncheck this check box so that the media stream is not encrypted.
SIP Transport Protocol	Select the SIP transport protocol that Cisco Unity Connection will use.
IPv4 Address or Host Name <i>(Unity Connection 10.0)</i>	<p>Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.</p> <p>You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.</p>

Table 3-25 Settings for the New Port Group Page (continued)

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

- Step 10** On the Port Group Basics page, do the following substeps if the Cisco Unified CM cluster has secondary servers, or if you want to add a TFTP server (required for Cisco Unified CM authentication and encryption). Otherwise, skip to [Step 11](#).
- On the Edit menu, select **Servers**.
 - If you want to add a secondary Cisco Unified CM server, on the Edit Servers page, under SIP Servers, select **Add**. Otherwise, skip to [Step 10e](#).
 - Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

Table 3-26 Settings for the SIP Servers

Field	Setting
Order	Enter the order of priority for the Cisco Unified CM server. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IPv4 Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IPv4 address (or host name) of the secondary Cisco Unified CM server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IPv6 address (or host name) of the secondary Cisco Unified CM server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. Note IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.
IP Address or Host Name (<i>Unity Connection 10..0</i>)	Enter the IP address (or host name) of the secondary Cisco Unified CM server.

Table 3-26 Settings for the SIP Servers (continued)

Field	Setting
Port	Enter the IP port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.

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

Table 3-27 Settings for the TFTP Servers

Field	Setting
Order	Enter the order of priority for the TFTP server. The lowest number is the primary TFTP server, the higher numbers are the secondary servers.
IPv4 Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IPv4 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IPv6 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. Note IPv6 is supported for SIP integrations with Cisco Unified CM 9.0.
IP Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IP address (or host name) of the TFTP server.

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

Table 3-28 Settings for the New Port Page

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

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



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

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

Table 3-29 Settings for the Voice Messaging Ports

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

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

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



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

- In the Download Complete dialog box, select **Close**.
- Step 19** Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM system integration by doing the following substeps.
- Step 20** If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**. Otherwise, skip to [Step 24](#).
- Step 21** On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.
- Step 22** On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

Table 3-30 Settings for the Phone System Trunk

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

- Step 23** Repeat [Step 21](#) and [Step 22](#) for all remaining phone system trunks that you want to create.
- Step 24** In the Related Links drop-down list, select **Check Telephony Configuration** and select **Go** to confirm the phone system integration settings.
- If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.
- Step 25** In the Task Execution Results window, select **Close**.



Setting Up a Cisco Unified Communications Manager 6.x SIP Trunk Integration with Cisco Unity Connection

For detailed instructions for setting up a Cisco Unified Communications Manager 6.x SIP trunk integration with Cisco Unity Connection, see the following sections in this chapter:

- [Integration Tasks, page 4-1](#)
- [Requirements, page 4-2](#)
- [“Centralized Voice Messaging” section on page 4-3](#)
- [Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection, page 4-3](#)
- [Creating a New Integration with Cisco Unified Communications Manager, page 4-18](#)

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



Note

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

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

Integration Tasks

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

1. Review the system and equipment requirements to confirm that all phone system and Cisco Unity Connection server requirements have been met. See the [“Requirements” section on page 4-2](#).
2. Plan how the voice messaging ports will be used by Cisco Unity Connection. See [Chapter 2, “Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection.”](#)

3. Program Cisco Unified CM. See the “Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection” section on page 4-3.
4. Create the integration. See the “Creating a New Integration with Cisco Unified Communications Manager” section on page 4-18.



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

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

Requirements

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

Phone System

- Cisco Unified CM 6.x.
For details on compatible versions of Cisco Unified CM, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- For the Cisco Unified CM extensions, one of the following configurations:
 - (Best practice) Only SIP phones that support DTMF relay as described in RFC-2833.
 - Both SCCP phones and SIP phones.
Note that older SCCP phone models may require a Media Termination Point (MTP) to function correctly.
- A LAN connection in each location where you will plug the applicable phone into the network.
- For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Cisco Unified CM cluster without having to dial a trunk access code or prefix.

Cisco Unity Connection Server

- The applicable version of Cisco Unity Connection. For details on compatible versions of Cisco Unity Connection, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- 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.
- A license that enables the applicable number of voice messaging ports.

Centralized Voice Messaging

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

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

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

- **Cisco Unity Connection without a Unity Connection cluster**—Do the procedures in the “For Cisco Unity Connection Without a Unity Connection Cluster” section on page 4-3.
- **Cisco Unity Connection with a Unity Connection cluster configured**—Do the procedures in the “For Cisco Unity Connection with a Unity Connection Cluster Configured” section on page 4-9.

For Cisco Unity Connection Without a Unity Connection Cluster

Do the following procedures in the order given.



Note

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

To Create the SIP Trunk Security Profile

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

Table 4-1 Settings for the SIP Trunk Security Profile Configuration Page

Field	Setting
Name	Enter Unity Connection SIP Trunk Security Profile or another name.
Description	Enter SIP trunk security profile for Cisco Unity Connection or another description.

Table 4-1 Settings for the SIP Trunk Security Profile Configuration Page (continued)

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

Step 4 Select **Save**.

To Create the SIP Profile

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

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

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

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

Table 4-2 Settings for the SIP Profile Configuration Page

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

Step 5 Select **Save**.

To Create the SIP Trunk

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

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

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

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

Step 5 Under Device Information, enter the following settings.

Table 4-3 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk or another name.
Description	Enter SIP trunk for Cisco Unity Connection or another description.

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

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

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

Step 7 If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 8](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.

Step 8 Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.

Step 9 Under SIP Information, enter the following settings.

Table 4-5 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the Cisco Unity Connection SIP port to which Cisco Unified CM will connect.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “To Create the SIP Trunk Security Profile” procedure on page 4-3 . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.

Table 4-5 Settings for SIP Information on the Trunk Configuration Page (continued)

Field	Setting
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile” procedure on page 4-4 . For example, select “Cisco Unity Connection SIP Profile.”

Step 10 Adjust any other settings that are needed for your site.

Step 11 Select **Save**.

To Create a Route Pattern

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

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

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

Table 4-6 Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the SIP trunk that you created in the “To Create the SIP Trunk” procedure on page 4-5 . For example, select “Unity_Connection_SIP_Trunk.”

Step 4 Select **Save**.

To Create the Voice Mail Pilot

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

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

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

Table 4-7 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern” procedure on page 4-6 .
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.

Table 4-7 Settings for the Voice Mail Pilot Configuration Page (continued)

Field	Setting
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

To Set Up the Voice Mail Profile

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

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

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

Table 4-8 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot” procedure on page 4-6 .
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

To Set Up the Voice Mail Server Service Parameters

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

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

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

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 4-18.

(Optional) To Set Up SIP Digest Authentication

- Step 1** On the System menu, select **Security Profile > SIP Trunk Security Profile**.
- Step 2** On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile”](#) procedure on page 4-3.
- Step 3** On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.
- Step 4** Select **Save**.

(Optional) To Create the Application User

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

Table 4-9 Settings for the Application User Configuration Page

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.

Table 4-9 Settings for the Application User Configuration Page (continued)

Field	Setting
Presence Group	<p>Used with the Presence feature, the application user (for example, IPMASysUser) serves as the watcher because it requests status about the presence entity.</p> <p>If you want the application user to receive the status of the presence entity, make sure that the Application User Presence group is allowed to view the status of the Presence group that is applied to the directory number, as indicated in the Presence Group Configuration window.</p>
Accept Presence Subscription	Leave this check box unchecked.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Header Replacement	Leave this check box unchecked.
Available Devices	<p>This list box displays the devices that are available for association with this application user.</p> <p>To associate a device with this application user, select the device and select the Down arrow below this list box.</p> <p>If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices:</p> <ul style="list-style-type: none"> • Find More Phones—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search. • Find More Route Points—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.
Groups	This list box appears after an application user has been added. The list box displays the groups to which the application user belongs.
Roles	This list box appears after an application user has been added. The list box displays the roles that are assigned to the application user.

Step 4 Select **Save**.

For Cisco Unity Connection with a Unity Connection Cluster Configured

Do the following procedures in the order given.

**Note**

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

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

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

Table 4-10 Settings for the SIP Trunk Security Profile Configuration Page

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

Step 4 Select **Save**.

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

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

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

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

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

Table 4-11 Settings for the SIP Profile Configuration Page

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

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

Step 6 Select **Save**.

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

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

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

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

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

Step 5 Under Device Information, enter the following settings.

Table 4-12 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_1 or another name.
Description	Enter SIP trunk 1 for Cisco Unity Connection or another description.

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

Table 4-13 Settings for Inbound Calls on the Trunk Configuration Page

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

- Step 7** If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 8](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.
- Step 8** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.
- Step 9** Under SIP Information, enter the following settings.

Table 4-14 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the publisher Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “ To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster) ” procedure on page 4-10. For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “ To Create the SIP Profile (for a Cisco Unity Connection Cluster) ” procedure on page 4-11. For example, select “Cisco Unity Connection SIP Profile.”

- Step 10** Adjust any other settings that are needed for your site.
- Step 11** Select **Save**.
- Step 12** Select **Add New**.
- Step 13** On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.
- Step 14** In the Device Protocol field, select **SIP** and select **Next**.
- Step 15** Under Device Information, enter the following settings.

Table 4-15 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_2 or another name.
Description	Enter SIP trunk 2 for Cisco Unity Connection or another description.

- Step 16** If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to [Step 17](#).

Table 4-16 Settings for Inbound Calls on the Trunk Configuration Page

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

- Step 17** If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 18](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.
- Step 18** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.
- Step 19** Under SIP Information, enter the following settings.

Table 4-17 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the subscriber Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “ To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster) ” procedure on page 4-10. For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “ To Create the SIP Profile (for a Cisco Unity Connection Cluster) ” procedure on page 4-11. For example, select “Cisco Unity Connection SIP Profile.”

- Step 20** Adjust any other settings that are needed for your site.
- Step 21** Select **Save**.

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

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

Table 4-18 Settings for the Route Group Configuration Page

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

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

Step 7 Select **Save**.

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

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

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

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

Table 4-19 Settings for the Route List Configuration Page

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

Step 4 Select **Save**.

Step 5 Confirm that the **Enable This Route List** check box is checked.

Step 6 Under Route List Member Information, select **Add Route Group**.

Step 7 On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the [“To Create a Route Group \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 4-13 and select **Save**.

Step 8 When prompted that the route list settings will be saved, select **OK**.

Step 9 On the Route List Configuration page, select **Reset**.

Step 10 When prompted to confirm resetting the route list, select **Reset**.

Step 11 Select **Close**.

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

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

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

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

Table 4-20 Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the SIP trunk that you created in the “To Create a Route List (for a Cisco Unity Connection Cluster)” procedure on page 4-14. For example, select “SIP_Trunk_Route_List.”

Step 4 Select **Save**.

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

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

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

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

Table 4-21 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern (for a Cisco Unity Connection Cluster)” procedure on page 4-14.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

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

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

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

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

Table 4-22 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot (for a Cisco Unity Connection Cluster)” procedure on page 4-15.

Table 4-22 Settings for the Voice Mail Profile Configuration Page (continued)

Field	Setting
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 4-18.

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

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

Step 2 On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 4-10.

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

Step 4 Select **Save**.

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

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

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

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

Table 4-23 Settings for the Application User Configuration Page

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

Step 4 Select **Save**.


Creating a New Integration with Cisco Unified Communications Manager

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

To Create an Integration

- Step 1** Sign in to Cisco Unity Connection Administration.
- Step 2** If you will use Cisco Unified CM authentication and encryption, do the following substeps. Otherwise, skip to [Step 3](#).
- In Cisco Unity Connection Administration, expand **Telephony Integrations**, expand **Security**, then select **SIP Certificate**.
 - On the SIP Certificates page, select **Add New**.
 - On the New SIP Certificate page, enter the following settings for the SIP certificate and select **Save**.

Table 4-24 Settings for the New SIP Certificate Page

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

- Step 3** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.
- Step 4** On the Search Phone Systems page, under Display Name, select the name of the default phone system.
- Step 5** On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.
- Step 6** If you want to use this phone system as the default for TRaP connections so that administrators and users without voicemail boxes can record and playback through the phone in Cisco Unity Connection web applications, check the **Default TRAP Switch** check box. If you want to use another phone system as the default for TRaP connections, uncheck this check box.
- Step 7** Select **Save**.
- Step 8** On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.
- Step 9** On the New Port Group page, enter the applicable settings and select **Save**.

Table 4-25 Settings for the New Port Group Page

Field	Setting
Phone System	Select the name of the phone system that you entered in Step 5 .
Create From	Select Port Group Template and select SIP in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Authenticate with SIP Server	Check this check box if you want Cisco Unity Connection to authenticate with the Cisco Unified CM server.
Authentication User Name	Enter the name that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Authentication Password	Enter the password that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users will use to contact Cisco Unity Connection and that Cisco Unity Connection will use to register with the Cisco Unified CM server.
SIP Security Profile	Select the SIP security profile that Cisco Unity Connection will use.
SIP Certificate	<i>(Only when a secure TLS port is used)</i> Confirm that the applicable SIP certificate is selected.
Security Mode	<p><i>(Only when a secure TLS port is used)</i> Select the applicable security mode:</p> <ul style="list-style-type: none"> • Authenticated—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an secure TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. • Encrypted—The integrity and privacy of call-signaling messages will be ensured on this port because they will be connected to Cisco Unified CM through an secure TLS port, and the call-signaling messages will be encrypted. <p>The Security Mode setting on the Cisco Unity Connection server must match the Device Security Mode setting on the Cisco Unified CM server.</p>
Secure RTP	<i>(Only when a secure TLS port is used)</i> Check this check box so that the media stream (RTP) is encrypted. Uncheck this check box so that the media stream is not encrypted.
SIP Transport Protocol	Select the SIP transport protocol that Cisco Unity Connection will use.
IPv4 Address or Host Name <i>(Unity Connection 10.0)</i>	<p>Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.</p> <p>You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.</p>

Table 4-25 Settings for the New Port Group Page (continued)

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

- Step 10** On the Port Group Basics page, do the following substeps if the Cisco Unified CM cluster has secondary servers, or if you want to add a TFTP server (required for Cisco Unified CM authentication and encryption). Otherwise, skip to [Step 11](#).
- On the Edit menu, select **Servers**.
 - If you want to add a secondary Cisco Unified CM server, on the Edit Servers page, under SIP Servers, select **Add**. Otherwise, skip to [Step 10e](#).
 - Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

Table 4-26 Settings for the SIP Servers

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

Table 4-26 Settings for the SIP Servers (continued)

Field	Setting
Port	Enter the IP port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.

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

Table 4-27 Settings for the TFTP Servers

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

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

Table 4-28 Settings for the New Port Page

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

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



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

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

Table 4-29 Settings for the Voice Messaging Ports

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

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

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



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

- In the Download Complete dialog box, select **Close**.
- Step 19** Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM system integration by doing the following substeps.
- Step 20** If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**. Otherwise, skip to [Step 24](#).
- Step 21** On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.
- Step 22** On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

Table 4-30 Settings for the Phone System Trunk

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

- Step 23** Repeat [Step 21](#) and [Step 22](#) for all remaining phone system trunks that you want to create.
- Step 24** In the Related Links drop-down list, select **Check Telephony Configuration** and select **Go** to confirm the phone system integration settings.
- If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.
- Step 25** In the Task Execution Results window, select **Close**.



Setting Up a Cisco Unified Communications Manager 7.x SIP Trunk Integration with Cisco Unity Connection

For detailed instructions for setting up a Cisco Unified Communications Manager 7.x SIP trunk integration with Cisco Unity Connection, see the following sections in this chapter:

- [Integration Tasks, page 5-1](#)
- [Requirements, page 5-2](#)
- [Centralized Voice Messaging, page 5-3](#)
- [.Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection, page 5-3](#)
- [Creating a New Integration with Cisco Unified Communications Manager, page 5-18](#)

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



Note

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

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

Integration Tasks

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

1. Review the system and equipment requirements to confirm that all phone system and Cisco Unity Connection server requirements have been met. See the [“Requirements” section on page 5-2](#).
2. Plan how the voice messaging ports will be used by Cisco Unity Connection. See [Chapter 2, “Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection.”](#)

3. Program Cisco Unified CM. See the “[Programming the Cisco Unified CallManager Phone System for Integrating with Cisco Unity Connection](#)” section on page 5-3.
4. Create the integration. See the “[Creating a New Integration with Cisco Unified Communications Manager](#)” section on page 5-18.



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

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

Requirements

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

Phone System

- Cisco Unified CM 7.x.

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

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

Note that older SCCP phone models may require a Media Termination Point (MTP) to function correctly.

- A LAN connection in each location where you will plug the applicable phone into the network.
- For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Cisco Unified CM cluster without having to dial a trunk access code or prefix.

Cisco Unity Connection Server

- The applicable version of Cisco Unity Connection. For details on compatible versions of Cisco Unity Connection, see the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- 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.
- A license that enables the applicable number of voice messaging ports.

Centralized Voice Messaging

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

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

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

- **Cisco Unity Connection without a Unity Connection cluster**—Do the procedures in the “For Cisco Unity Connection Without a Unity Connection Cluster” section on page 5-3.
- **Cisco Unity Connection with a Unity Connection cluster configured**—Do the procedures in the “For Cisco Unity Connection with a Unity Connection Cluster Configured” section on page 5-9.

For Cisco Unity Connection Without a Unity Connection Cluster

Do the following procedures in the order given.



Note

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

To Create the SIP Trunk Security Profile

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

Table 5-1 Settings for the SIP Trunk Security Profile Configuration Page

Field	Setting
Name	Enter Unity Connection SIP Trunk Security Profile or another name.
Description	Enter SIP trunk security profile for Cisco Unity Connection or another description.

Table 5-1 Settings for the SIP Trunk Security Profile Configuration Page (continued)

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

Step 4 Select **Save**.

To Create the SIP Profile

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

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

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

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

Table 5-2 Settings for the SIP Profile Configuration Page

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

Step 5 Select **Save**.

To Create the SIP Trunk

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

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

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

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

Step 5 Under Device Information, enter the following settings.

Table 5-3 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk or another name.
Description	Enter SIP trunk for Cisco Unity Connection or another description.

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

Table 5-4 Settings for Inbound Calls on the Trunk Configuration Page

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

Step 7 If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 8](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.

Step 8 Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.

Step 9 Under SIP Information, enter the following settings.

Table 5-5 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the Cisco Unity Connection SIP port to which Cisco Unified CM will connect.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “To Create the SIP Trunk Security Profile” procedure on page 5-3 . For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.

Table 5-5 Settings for SIP Information on the Trunk Configuration Page (continued)

Field	Setting
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “To Create the SIP Profile” procedure on page 5-4 . For example, select “Cisco Unity Connection SIP Profile.”

Step 10 Adjust any other settings that are needed for your site.

Step 11 Select **Save**.

To Create a Route Pattern

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

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

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

Table 5-6 Settings for the Route Pattern Configuration Page

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

Step 4 Select **Save**.

To Create the Voice Mail Pilot

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

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

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

Table 5-7 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern” procedure on page 5-6 .
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.

Table 5-7 Settings for the Voice Mail Pilot Configuration Page (continued)

Field	Setting
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

To Set Up the Voice Mail Profile

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

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

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

Table 5-8 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot” procedure on page 5-6 .
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

To Set Up the Voice Mail Server Service Parameters

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

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

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

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 5-18.

(Optional) To Set Up SIP Digest Authentication

- Step 1** On the System menu, select **Security Profile > SIP Trunk Security Profile**.
- Step 2** On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile”](#) procedure on page 5-3.
- Step 3** On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.
- Step 4** Select **Save**.

(Optional) To Create the Application User

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

Table 5-9 Settings for the Application User Configuration Page

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.

Table 5-9 Settings for the Application User Configuration Page (continued)

Field	Setting
Presence Group	<p>Used with the Presence feature, the application user (for example, IPMASysUser) serves as the watcher because it requests status about the presence entity.</p> <p>If you want the application user to receive the status of the presence entity, make sure that the Application User Presence group is allowed to view the status of the Presence group that is applied to the directory number, as indicated in the Presence Group Configuration window.</p>
Accept Presence Subscription	Leave this check box unchecked.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Header Replacement	Leave this check box unchecked.
Available Devices	<p>This list box displays the devices that are available for association with this application user.</p> <p>To associate a device with this application user, select the device and select the Down arrow below this list box.</p> <p>If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices:</p> <ul style="list-style-type: none"> • Find More Phones—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search. • Find More Route Points—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.
Groups	This list box appears after an application user has been added. The list box displays the groups to which the application user belongs.
Roles	This list box appears after an application user has been added. The list box displays the roles that are assigned to the application user.

Step 4 Select **Save**.

For Cisco Unity Connection with a Unity Connection Cluster Configured

Do the following procedures in the order given.

**Note**

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

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

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

Table 5-10 Settings for the SIP Trunk Security Profile Configuration Page

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

Step 4 Select **Save**.

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

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

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

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

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

Table 5-11 Settings for the SIP Profile Configuration Page

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

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

Step 6 Select **Save**.

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

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

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

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

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

Step 5 Under Device Information, enter the following settings.

Table 5-12 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_1 or another name.
Description	Enter SIP trunk 1 for Cisco Unity Connection or another description.

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

Table 5-13 Settings for Inbound Calls on the Trunk Configuration Page

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

- Step 7** If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 8](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.
- Step 8** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.
- Step 9** Under SIP Information, enter the following settings.

Table 5-14 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the publisher Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “ To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster) ” procedure on page 5-10. For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “ To Create the SIP Profile (for a Cisco Unity Connection Cluster) ” procedure on page 5-11. For example, select “Cisco Unity Connection SIP Profile.”

- Step 10** Adjust any other settings that are needed for your site.
- Step 11** Select **Save**.
- Step 12** Select **Add New**.
- Step 13** On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.
- Step 14** In the Device Protocol field, select **SIP** and select **Next**.
- Step 15** Under Device Information, enter the following settings.

Table 5-15 Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter Unity_Connection_SIP_Trunk_2 or another name.
Description	Enter SIP trunk 2 for Cisco Unity Connection or another description.

- Step 16** If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to [Step 17](#).

Table 5-16 Settings for Inbound Calls on the Trunk Configuration Page

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

- Step 17** If you will not enable Cisco Unified CM authentication and encryption, continue to [Step 18](#). If you will enable Cisco Unified CM authentication and encryption, check the **SRTP Allowed** check box.
- Step 18** Under Outbound Calls, check the **Redirecting Diversion Header Delivery - Outbound** check box.
- Step 19** Under SIP Information, enter the following settings.

Table 5-17 Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the subscriber Cisco Unity Connection server.
Destination Port	We recommend that you accept the default of 5060 .
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the “ To Create the SIP Trunk Security Profile (for a Cisco Unity Connection Cluster) ” procedure on page 5-10. For example, select “Cisco Unity Connection SIP Trunk Security Profile.”
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the “ To Create the SIP Profile (for a Cisco Unity Connection Cluster) ” procedure on page 5-11. For example, select “Cisco Unity Connection SIP Profile.”

- Step 20** Adjust any other settings that are needed for your site.
- Step 21** Select **Save**.

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

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

Table 5-18 Settings for the Route Group Configuration Page

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

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

Step 7 Select **Save**.

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

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

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

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

Table 5-19 Settings for the Route List Configuration Page

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

Step 4 Select **Save**.

Step 5 Confirm that the **Enable This Route List** check box is checked.

Step 6 Under Route List Member Information, select **Add Route Group**.

Step 7 On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the [“To Create a Route Group \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 5-13 and select **Save**.

Step 8 When prompted that the route list settings will be saved, select **OK**.

Step 9 On the Route List Configuration page, select **Reset**.

Step 10 When prompted to confirm resetting the route list, select **Reset**.

Step 11 Select **Close**.

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

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

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

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

Table 5-20 Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Cisco Unity Connection.
Gateway/Route List	Select the name of the route list that you created in the “To Create a Route List (for a Cisco Unity Connection Cluster)” procedure on page 5-14. For example, select “SIP_Trunk_Route_List.”

Step 4 Select **Save**.

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

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

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

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

Table 5-21 Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users will dial to listen to their voice messages. This number must match the route pattern that you entered in the “To Create a Route Pattern (for a Cisco Unity Connection Cluster)” procedure on page 5-14.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter Unity Connection Pilot or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

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

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

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

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

Table 5-22 Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter Unity Connection Profile or another name to identify the voice mail profile.
Description	Enter Profile for Cisco Unity Connection or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the “To Create the Voice Mail Pilot (for a Cisco Unity Connection Cluster)” procedure on page 5-15.

Table 5-22 Settings for the Voice Mail Profile Configuration Page (continued)

Field	Setting
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

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

If you do not want to set up SIP digest authentication, continue to the [“Creating a New Integration with Cisco Unified Communications Manager”](#) section on page 5-18.

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

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

Step 2 On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the [“To Create the SIP Trunk Security Profile \(for a Cisco Unity Connection Cluster\)”](#) procedure on page 5-10.

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

Step 4 Select **Save**.

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

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

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

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

Table 5-23 Settings for the Application User Configuration Page

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

Step 4 Select **Save**.


Creating a New Integration with Cisco Unified Communications Manager

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

To Create an Integration

- Step 1** Sign in to Cisco Unity Connection Administration.
- Step 2** If you will use Cisco Unified CM authentication and encryption, do the following substeps. Otherwise, skip to [Step 3](#).
- In Cisco Unity Connection Administration, expand **Telephony Integrations**, expand **Security**, then select **SIP Certificate**.
 - On the SIP Certificates page, select **Add New**.
 - On the New SIP Certificate page, enter the following settings for the SIP certificate and select **Save**.

Table 5-24 Settings for the New SIP Certificate Page

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

- Step 3** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.
- Step 4** On the Search Phone Systems page, under Display Name, select the name of the default phone system.
- Step 5** On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.
- Step 6** If you want to use this phone system as the default for TRaP connections so that administrators and users without voicemail boxes can record and playback through the phone in Cisco Unity Connection web applications, check the **Default TRAP Switch** check box. If you want to use another phone system as the default for TRaP connections, uncheck this check box.
- Step 7** Select **Save**.
- Step 8** On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.
- Step 9** On the New Port Group page, enter the applicable settings and select **Save**.

Table 5-25 Settings for the New Port Group Page

Field	Setting
Phone System	Select the name of the phone system that you entered in Step 5 .
Create From	Select Port Group Template and select SIP in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Authenticate with SIP Server	Check this check box if you want Cisco Unity Connection to authenticate with the Cisco Unified CM server.
Authentication User Name	Enter the name that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Authentication Password	Enter the password that Cisco Unity Connection will use to authenticate with the Cisco Unified CM server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users will use to contact Cisco Unity Connection and that Cisco Unity Connection will use to register with the Cisco Unified CM server.
SIP Security Profile	Select the SIP security profile that Cisco Unity Connection will use.
SIP Certificate	<i>(Only when a secure TLS port is used)</i> Confirm that the applicable SIP certificate is selected.
Security Mode	<p><i>(Only when a secure TLS port is used)</i> Select the applicable security mode:</p> <ul style="list-style-type: none"> • Authenticated—The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an secure TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. • Encrypted—The integrity and privacy of call-signaling messages will be ensured on this port because they will be connected to Cisco Unified CM through an secure TLS port, and the call-signaling messages will be encrypted. <p>The Security Mode setting on the Cisco Unity Connection server must match the Device Security Mode setting on the Cisco Unified CM server.</p>
Secure RTP	<i>(Only when a secure TLS port is used)</i> Check this check box so that the media stream (RTP) is encrypted. Uncheck this check box so that the media stream is not encrypted.
SIP Transport Protocol	Select the SIP transport protocol that Cisco Unity Connection will use.
IPv4 Address or Host Name <i>(Unity Connection 10.0)</i>	<p>Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.</p> <p>You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.</p>

Table 5-25 Settings for the New Port Group Page (continued)

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

- Step 10** On the Port Group Basics page, do the following substeps if the Cisco Unified CM cluster has secondary servers, or if you want to add a TFTP server (required for Cisco Unified CM authentication and encryption). Otherwise, skip to [Step 11](#).
- On the Edit menu, select **Servers**.
 - If you want to add a secondary Cisco Unified CM server, on the Edit Servers page, under SIP Servers, select **Add**. Otherwise, skip to [Step 10e](#).
 - Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

Table 5-26 Settings for the SIP Servers

Field	Setting
Order	Enter the order of priority for the Cisco Unified CM server. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IPv4 Address or Host Name (<i>Unity Connection</i>)	Enter the IPv4 address (or host name) of the secondary Cisco Unified CM server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IPv6 address (or host name) of the secondary Cisco Unified CM server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. Note IPv6 is supported for SIP integrations with Cisco Unified CM 9.0.
IP Address or Host Name (<i>Unity Connection 10.0</i>)	Enter the IP address (or host name) of the secondary Cisco Unified CM server.

Table 5-26 Settings for the SIP Servers (continued)

Field	Setting
Port	Enter the IP port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Cisco Unity Connection. We recommend that you use the default setting.

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

Table 5-27 Settings for the TFTP Servers

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

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

Table 5-28 Settings for the New Port Page

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

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



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

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

Table 5-29 Settings for the Voice Messaging Ports

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

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

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



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

- In the Download Complete dialog box, select **Close**.
- Step 19** Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM system integration by doing the following substeps.
- Step 20** If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**. Otherwise, skip to [Step 24](#).
- Step 21** On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.
- Step 22** On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

Table 5-30 Settings for the Phone System Trunk

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

- Step 23** Repeat [Step 21](#) and [Step 22](#) for all remaining phone system trunks that you want to create.
- Step 24** In the Related Links drop-down list, select **Check Telephony Configuration** and select **Go** to confirm the phone system integration settings.
- If the test is not successful, the Task Execution Results displays one or more messages with troubleshooting steps. After correcting the problems, test the connection again.
- Step 25** In the Task Execution Results window, select **Close**.



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

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

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

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



Note

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

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

Integration Tasks

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

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

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



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

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

Requirements

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

Phone System

- Cisco Unified CM 10.x

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

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

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

Cisco Unity Connection Server

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

- 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.
- A license that enables the applicable number of voice messaging ports.

Centralized Voice Messaging

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

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

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

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

For Cisco Unity Connection Without a Unity Connection Cluster

Revised April 17, 2014

Do the following procedures in the order given.



Note

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

To Create the SIP Trunk Security Profile

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

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

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

Step 4 Select **Save**.

To Create the SIP Profile

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

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

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

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

Table 6-2 Settings for the SIP Profile Configuration Page

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

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

Step 6 Select **Save**.

To Create the SIP Trunk

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

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

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

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

Step 5 Under Device Information, enter the following settings.

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

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

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

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

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

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

Table 6-5 Settings Outbound Calls on Trunk Configuration Page

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

Step 8 Under SIP Information, enter the following settings.

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

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

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

Step 10 Select **Save**.

To Create a Route Pattern

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

- Step 2** On the Find and List Route Patterns page, select **Add New**.
- Step 3** On the Route Pattern Configuration page, enter the following settings.

Table 6-7 Settings for the Route Pattern Configuration Page

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

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

To Create the Voice Mail Pilot

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

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

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

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

To Set Up the Voice Mail Profile

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

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

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

Step 4 Select **Save**.

To Set Up the Voice Mail Server Service Parameters

- Step 1** In Cisco Unified CM Administration, select **System > Service Parameters**.
- Step 2** On the Service Parameters Configuration page, in the Server field, select the name of the Cisco Unified CM server.
- Step 3** In the Service list, select **Cisco CallManager**. The list of parameters appears.
- Step 4** Under Clusterwide Parameters (Feature - General), locate the Multiple Tenant MWI Modes parameter.
- Step 5** If you use multiple tenant MWI notification, select **True**.

When this parameter is set to True, Cisco Unified CM uses any configured translation patterns to convert voicemail extensions into directory numbers when turning on or off an MWI.
- Step 6** If you changed any settings, select **Save**. Then shut down and restart the Cisco Unified CM server.
-

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

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

(Optional) To Set Up SIP Digest Authentication

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

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

(Optional) To Create the Application User

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

Table 6-10 Settings for the Application User Configuration Page

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

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

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

Step 4 Select **Save**.

For Cisco Unity Connection with a Unity Connection Cluster Configured

Do the following procedures in the order given.



Note

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

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

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

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

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

Step 4 Select **Save**.

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

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

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

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

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

Table 6-12 Settings for the SIP Profile Configuration Page

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

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

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

Step 7 Select **Save**.

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

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

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

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

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

Step 5 Under Device Information, enter the following settings.

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

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

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

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

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

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

Step 8 Under SIP Information, enter the following settings.

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

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

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

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

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

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

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

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

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

Step 17 Under SIP Information, enter the following settings.

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

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

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

Step 19 Select **Save**.

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

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

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

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

Table 6-19 Settings for the Route Group Configuration Page

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

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

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

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

Table 6-20 Settings for the Route List Configuration Page

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

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

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

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

Table 6-21 Settings for the Route Pattern Configuration Page

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

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

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

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

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

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

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

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

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

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

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

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

Step 4 Select **Save**.

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

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

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

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

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

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

Step 4 Select **Save**.

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

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

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

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

Table 6-24 Settings for the Application User Configuration Page

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

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

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

Step 4 Select **Save**.

Creating a New Integration with Cisco Unified Communications Manager

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


To Create an Integration

Step 1 Sign in to Cisco Unity Connection Administration.

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

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

Table 6-25 Settings for the New SIP Certificate Page

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

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

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

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

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

Table 6-26 Settings for the New Port Group Page

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

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

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

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

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

Table 6-27 Settings for the SIP Servers

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

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

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

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

Table 6-28 Settings for the TFTP Servers

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

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

Table 6-29 Settings for the New Port Page

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

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



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

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

Table 6-30 Settings for the Voice Messaging Ports

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

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

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



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

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

Table 6-31 Settings for the Phone System Trunk

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

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

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

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



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, see the following documentation as applicable:

- The installation guide for the phone system.
- *Troubleshooting Guide for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx.html.
- 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** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.
- Step 4** On the Search Users page, select the display name of a user to use for testing. The extension for this user must be the extension for Phone 1.
- Step 5** On the Edit User Basics page, uncheck the **Set for Self-enrollment at Next Login** check box.
- Step 6** In the Voice Name field, record a recorded name for the test user.
- Step 7** Select **Save**.
- Step 8** On the Edit menu, select **Message Waiting Indicators**.
- Step 9** On the Message Waiting Indicators page, select the message waiting indicator. If no message waiting indication is in the table, select **Add New**.
- Step 10** On the Edit Message Waiting Indicator page, enter the following settings.

Table 7-1 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 11** Select **Save**.
- Step 12** On the Edit menu, select **Transfer Options**.
- Step 13** On the Transfer Options page, select the active option.
- Step 14** On the Edit Transfer Option page, under Transfer Action, select the **Extension** option and enter the extension of Phone 1.
- Step 15** In the Transfer Type field, select **Release to Switch**.
- Step 16** Select **Save**.
- Step 17** 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 18** Sign in to the Real-Time Monitoring Tool (RTMT).
- Step 19** On the Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.
- Step 20** In the right pane, select **Start Polling**. The Port Monitor will display which port is handling 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 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 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 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 name for the test user (if you did not record a name for the test user, you will hear the extension number for Phone 1). Hearing the recorded 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 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, select **Supervise Transfer**.
- Step 2** In the Rings to Wait For field, enter **3**.
- Step 3** Select **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 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 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** Select **Stop Polling**.
 - Step 10** Exit RTMT.
-

To Delete the Test User

- Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.
 - Step 2** On the Search Users page, check the check box to the left of the test user.
 - Step 3** Select **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.
-



Adding New User Templates for Multiple Integrations

When you create the first phone system integration, this first 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, or on selecting a user template when adding a new user, see the “User Templates” section in “User Attributes” chapter of the *System Administration Guide for Cisco Unity Connection Release 10.x*. The guide is available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx/10xcucsag030.html.



Adding Cisco Unified Communications Manager Express to a Cisco Unified Communications Manager Integration

Cisco Unity Connection can integrate a Cisco Unified Communications Manager phone system integration that has a port group of Cisco Unified CM servers and a Cisco Unified Communications Manager 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 Connection must be a supported combination in the *SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express* at http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- 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** Sign in to Cisco Unity Connection Administration.
- Step 2** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.
- Step 3** On the Search Port Groups page, select the name of the port group for the Cisco Unified CM servers.
- Step 4** On the Port Group Basics page, on the Edit menu, select **Servers**.
- Step 5** On the Edit Servers page, under Cisco Unified Communications Manager, select **Add**.
- Step 6** In the new row, enter the following settings.

Table 9-1 Settings for the Cisco Unified CM Express Server

Field	Setting
Order	Enter a number that is higher than the Cisco Unified CM servers. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IPv4 Address or Host Name)	Enter the IPv4 address (or host name) of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group.
IPv6 Address or Host Name)	Do not use this field for Cisco Unified CM Express integrations. IPv6 is not supported between Cisco Unity Connection and Cisco Unified CM Express.
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.

- Step 7** Select **Save**.
- Step 8** On the Edit menu, select **Advanced Settings**.
- Step 9** On the Edit Advanced Settings page, in the Delay After Answer field, enter **1000** and select **Save**.
- Step 10** On the Edit menu, select **Port Group Basics**.
- Step 11** On the Port Group Basics page, select **Reset**.
- Step 12** When prompted that resetting will terminate all call traffic, select **OK**.
- Step 13** In the Related Links drop-down list, select **Test Port Group** and select **Go** to confirm the Cisco Unified CM Express port group settings.
- Step 14** When prompted that the test will terminate call in progress, select **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 15** In the Task Execution Results window, select **Close**.
- Step 16** Sign out of Cisco Unity Connection Administration.



A

Allow TRAP Connections (port setting) [2-2](#)

Answer Calls (port setting) [2-2](#)

C

call information [1-1](#)

Cisco Unified CM 6.x

requirements [4-2](#)

task list, creating a SIP trunk integration [4-1](#)

E

Enabled (port setting) [2-2](#)

F

forwarded calls, information sent by phone system [1-1](#)

M

multiple integrations

adding new user template [8-1](#)

P

Perform Message Notification (port setting) [2-2](#)

ports

considerations for Cisco Unity Connection cluster [2-3](#)

planning how many will answer calls [2-3](#)

planning how many will dial out [2-3](#)

planning number to install [2-2](#)

planning setup [2-1](#)

settings [2-2](#)

S

Send MWI Requests (port setting) [2-2](#)

Server Name (port setting) [2-2](#)

T

template, adding a new user template for multiple integrations [8-1](#)

testing

deleting the test user [7-4](#)

setting up supervised transfer [7-3](#)

setting up test configuration [7-1](#)

testing an external call with release transfer [7-2](#)

testing supervised transfer [7-3](#)

testing the functionality for listening to messages [7-3](#)

U

user template, adding new for multiple integrations [8-1](#)

V

voice messaging ports, settings [2-2](#)

