



## **Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 14**

**First Published:** 2020-11-25

**Last Modified:** 2020-11-25

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## CONTENTS

---

### CHAPTER 1

#### **Integration Overview 1**

- Integration Overview 1
- Introduction 1
- Call Information 1
- Integration Functionality 2
- Integrations with Multiple Phone Systems 2
- Centralized Voice Messaging 2

---

### CHAPTER 2

#### **Planning the Voice Messaging Ports 3**

- Planning the Voice Messaging Ports 3
  - Planning the Port Setup 3
  - Determining the Number of Voice Messaging Ports 3
    - Voice Messaging Ports to Install 4
    - Voice Messaging Ports to Answer Calls 4
    - Voice Messaging Ports to Dial Out 4
  - Considerations for a Unity Connection Cluster 5
    - When Both Unity Connection Servers are Functioning 5
    - When Only One Unity Connection Server is Functioning 5

---

### CHAPTER 3

#### **Setting Up a Cisco Unified Communications Manager SCCP Integration 7**

- Setting Up a Cisco Unified Communications Manager SCCP Integration 7
  - Introduction 7
  - Pre-requisites 7
  - Integration Tasks 10
  - Programming the Cisco Unified CallManager Phone System 10
    - Adding Partitions and a Calling Search Space for Voice Mail Ports 10

Adding a Device Pool for the Voice Mail Ports 11

Adding the Voice Mail Ports on Cisco Unified CM 12

Adding the Answering Voice Mail Ports to a Line Group 14

Adding the Line Group to a Hunt List 15

Adding the Hunt List to a Hunt Pilot Number 16

Specifying the MWI Directory Numbers 17

Add a Voice Mail Pilot Number for the Voice Mail Ports 18

Setting Up the Voice Mail Profile 19

Setting Up the Voice Mail Server Service Parameters 19

Creating a New Integration with Cisco Unified CM 20

---

**CHAPTER 4**

**Configuring Voice Messaging Ports Configuration for a Unity Connection Cluster 31**

Configuring Voice Messaging Ports Configuration for a Unity Connection Cluster 31

Introduction 31

Voice Messaging Port for Unity Connection Cluster 31

Voice Messaging Ports Configuration for a Unity Connection Cluster 32

---

**CHAPTER 5**

**Testing the Integration 33**

Testing the Telephony Integration 33

Setting Up the Test Configuration 34

Testing an External Call with Release Transfer 35

Testing Listening to Messages 35

Setting Up Supervised Transfer on Cisco Unity Connection 36

Testing Supervised Transfer 36

Deleting the Test User 36

Testing Cisco Unified CM Authentication and Encryption 37

---

**CHAPTER 6**

**Changing the Number of Voice Messaging Ports 39**

Changing the Number of Voice Messaging Ports 39

Introduction 39

Adding Voice Messaging Ports 39

Deleting Voice Messaging Ports 40

---

**CHAPTER 7**

**Cisco Unified Communications Manager Authentication and Encryption 43**

Cisco Unified Communications Manager Authentication and Encryption 43

Introduction 43

Cisco Unified CM Security Features 43

---

**CHAPTER 8**

**Adding Cisco Unified Communications Manager Express to a Cisco Unified Communications Manager Integration 47**

Adding Cisco Unified Communications Manager Express to a Cisco Unified Communications Manager Integration 47

Overview 47

Adding Cisco Unified CM Express Server to Cisco Unified CM Phone System Integration 47

Use of Cisco Unified Survivable Remote Site Telephony (SRST) Router 48

Impact of Non-Delivery of RDNIS on Voice Mail Calls Routed via AAR 49





# CHAPTER 1

## Integration Overview

---

- [Integration Overview, on page 1](#)
- [Introduction, on page 1](#)
- [Call Information, on page 1](#)
- [Integration Functionality, on page 2](#)
- [Integrations with Multiple Phone Systems, on page 2](#)
- [Centralized Voice Messaging, on page 2](#)

## Integration Overview

### Introduction

The SCCP trunk integration is a method to establish communication between Unity Connection and Cisco Unified Communications Manager Express using SIP protocol. The Cisco Unified CM SCCP 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 by SCCP, see the Compatibility Matrix for Cisco Unity Connection at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/compatibility/matrix/b\\_cucclientmtx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html).

This document applies only when Unity Connection is installed on a separate server from Cisco Unified CM. This document does not apply to the configuration in which Unity Connection is installed as CiscoBusiness 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)

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

## Integration Functionality

The Cisco Unified CM SCCP integration with 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; Unity Connection identifies a user based on the extension from which the call originated; a password may be required)
- Identified user messaging (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)

## Integrations with Multiple Phone Systems

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 Unity Connection with multiple phone systems, see the *Multiple Phone System Integration Guide for Cisco Unity Connection, Release 14* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/integration/multiple/b\\_cuc14intmultiple.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/multiple/b_cuc14intmultiple.html).

## 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 supports 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 14 at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/design/guide/b\\_14cucdg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/design/guide/b_14cucdg.html).





## CHAPTER 2

# Planning the Voice Messaging Ports

---

- [Planning the Voice Messaging Ports, on page 3](#)

## Planning the Voice Messaging Ports

### Planning the Port Setup

Before programming the phone system, you need to plan how the voice messaging ports are going to be used by Cisco Unity Connection. The following considerations 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 Unity Connection cluster, each Unity Connection server must have enough ports to handle all voice messaging traffic in case the other server stops functioning. The Cisco Unified CM server must have enough ports installed for all Unity Connection servers.

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

### Determining the Number of Voice Messaging Ports

The following tasks describe the process for determining the number of voice messaging ports for Cisco Unity Connection to install, answer call and dial out calls:

- For determining the number of voice messaging ports to Install, see “[Voice Messaging Ports to Install](#)” section.
- For determining the number of voice messaging ports to Answer Calls, see “[Voice Messaging Ports to Answer Calls](#)” section.
- For determining the number of voice messaging ports to Dial Out, see “[Voice Messaging Ports to Dial Out](#)” section.

## Voice Messaging Ports to Install

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

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

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

If your system is configured for a Cisco Unity Connection cluster, see the [Considerations for a Unity Connection Cluster](#).

## Voice Messaging Ports to 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 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 Unity Connection Cluster](#).

## Voice Messaging Ports to Dial Out

Ports that only dial out and do 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 Unity Connection so that users can use the phone as a recording and playback device in 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 Unity Connection Cluster](#).

**Caution**

In programming the phone system, do not send calls to voice messaging ports in 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 Unity Connection Cluster

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

### When Both Unity Connection Servers are Functioning

- The phone system is provisioned with twice the number SCCP voice mail port devices needed to handle the voice messaging traffic.
- 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 Unity Connection servers are active and handle voice messaging traffic for the system.
- In Cisco Unity Connection Administration, the voice messaging ports are assigned in the following manner:
  - The subscriber server answers most incoming calls for the system.
  - The publisher server handles most dial-out calls (MWI requests and notifications).

This guide directs you to assign the voice messaging ports to their specific Unity Connection server at the applicable time.

- The voice messaging ports on both the servers are registered with the phone system.
- The number of voice messaging ports that are assigned to one 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 Unity Connection server stops functioning.

If both the Unity Connection servers are functioning to handle the voice messaging traffic, the system does not have sufficient capacity when one of the servers stops functioning.

- Each Unity Connection server is assigned half the total number of voice messaging ports.

If all the voice messaging ports are assigned to one Unity Connection server, the other Unity Connection server is not able to answer calls or to dial out.

- Each Unity Connection server must be assigned voice messaging ports that answer calls and that can dial out (for example, to set MWIs).

### When Only One Unity Connection Server is Functioning

- The SCCP voice mail port devices that have stopped functioning on the phone system are unregistered from the voice messaging ports of Unity Connection server.
- The hunt group on the phone system sends all calls to the functioning Unity Connection server.

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

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

All the ports for all Unity Connection servers must appear on the Search Ports page. Otherwise, the Unity Connection cluster has not been correctly configured and does not function correctly.



## CHAPTER 3

# Setting Up a Cisco Unified Communications Manager SCCP Integration

- [Setting Up a Cisco Unified Communications Manager SCCP Integration, on page 7](#)

## Setting Up a Cisco Unified Communications Manager SCCP Integration

### Introduction

This chapter provides instructions for setting up SCCP Integration between Cisco Unified Communications Manager and Cisco Unity Connection.



**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 Unity Connection settings.

### Pre-requisites

Before starting the SCCP integration between Cisco Unified CM and Unity Connection, you need to understand the tasks to be done and the components required for the integration. Below [Table 3-1](#) contains a list of pre-requisites that you must consider to ensure a successful integration.

Pre-requisites	Important Notes
Install the applicable version of Cisco Unified CM.	<ul style="list-style-type: none"><li>• For compatible version of Cisco Unified CM, see the <i>Compatibility Matrix: Cisco Unity Connection</i> <a href="#">Cisco Unified Communications Manager SCCP Integration, on page 7</a>.</li></ul>

<p>Install the applicable version of Unity Connection with a license that enables the applicable number of voice messaging ports.</p>	<ul style="list-style-type: none"> <li>• For details on compatible versions of Unity Connection, see the Compatibility Matrix for Cisco Unity Connection, available at <a href="http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support.html">http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support.html</a></li> <li>• For details on installation tasks, see the “Installing Cisco Unity Connection” chapter of the <i>Install, Maintenance Guide for Cisco Unity Connection</i>, Release 14, available at <a href="https://www.cisco.com/c/en/us/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html">https://www.cisco.com/c/en/us/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html</a></li> </ul>
<p>The supported Phone system for SCCP integration are:</p> <ul style="list-style-type: none"> <li>• Only IP phones for the Cisco Unified CM extensions.</li> <li>• Both IP phones and SIP phones for the Cisco Unified CM extensions without a media termination point (MTP) on the Cisco Unified CM server.</li> </ul>	<ul style="list-style-type: none"> <li>• A LAN connection in each location is required where you plug the applicable phone into the network.</li> <li>• For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Cisco Unified CM cluster without dialing a trunk access code or prefix.</li> </ul>

<p>If Unity Connection uses IPv6 or dual-mode (IPv4 and IPv6) to communicate with Cisco Unified CM, do the following subtasks:</p> <ol style="list-style-type: none"> <li>1. Enable IPv6 on the Unity Connection server.</li> <li>2. In Cisco Unity Connection Administration, on the <b>System Settings &gt; General Configuration</b> page, select an option for IP Addressing Mode to control where Unity Connection listens for incoming traffic. You can select IPv4, IPv6, or IPv4 and IPv6. The setting defaults to IPv4.</li> </ol>	<p>See the “Ethernet IPv6 Configuration Settings” section in the “Security” chapter of the Cisco Unified Operating System Administration Guide for Cisco Unity Connection at <a href="http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenan">http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenan</a></p>
---	--

## Integration Tasks

The following task list describes the process for creating and changing the integration.

1. Review the system and hardware requirements to confirm that all phone system and Unity Connection server requirements have been met. See the “[Pre-requisites](#)” section on page 3-1
2. Plan and configure how the voice messaging ports are used by Unity Connection. See [Planning the Port Setup](#)




---

**Note** All the forwarded calls are routed to opening greeting instead of subscriber greeting when Voice mail port, Voice mail pilot, and CTI route point used for routing calls to Unity Connection are same as that of Phone DN on call manager.

---

3. Program Cisco Unified CM. See the [Programming the Cisco Unified CallManager Phone System](#).
4. Create the integration. See the “[Creating a New Integration with Cisco Unified CM](#).”




---

**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 [Testing the Integration](#) chapter.




---

**Note** If this is the first integration, the first phone system is automatically selected in the default user template. The users that you add after creating this phone system integration are assigned to this phone system by default. However, for each subsequent integration add the applicable new user templates for 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 14 available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/administration/guide/b\\_14cucsag.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html).

---

## Programming the Cisco Unified CallManager Phone System

Do the following procedures for programming the Cisco Unified Communications Manager phone system integration with Unity Connection:

### Adding Partitions and a Calling Search Space for Voice Mail Ports

- 
- Step 1** In Cisco Unified CM Administration, expand **Call Routing** > **Class of Control** > **and select** > **Partition**.
- Step 2** On the Find and List Partitions page, select **Add New**.



- Step 3** On the Partition Configuration page, enter the name and description you want for the partition that contains all voice mail port directory numbers. For example, enter “VMRestrictedPT, Partition for voice mail port directory numbers.”
- Step 4** Select **Save**.
- Step 5** Select **Add New**.
- Step 6** Enter the name and description you want for the partition that contains the hunt pilot, which is the voice mail pilot number. For example, enter “VMPilotNumberPT, Partition for the voice mail pilot number.”
- Step 7** Select **Save**.
- Step 8** Expand **Call Routing > Class of Control > and select > Calling Search Space**.
- Step 9** On the Find and List Calling Search Spaces page, select **Add New**.
- Step 10** On the Calling Search Space Configuration page, in the Name field, enter a name for the calling search space that includes the partition created in [Step 2](#) through [Step 4](#). For example, enter “VMRestrictedCSS.”
- Step 11** Optionally, in the Description field, enter a description of the calling search space. For example, enter “Voice mail port directory numbers.”
- Step 12** In the Available Partitions list, select the name of the partition created in [Step 2](#) through [Step 4](#). For example, select “VMRestrictedPT.”
- Step 13** Select the down arrow below the Available Partitions list.  
The name of the partition appears in the Selected Partitions list.
- Step 14** Select **Save**.
- Step 15** In the Related Links field, select **Back to Find/List** and select **Go**.
- Step 16** On the Find and List Calling Search Spaces page, select **Find**.
- Step 17** Select the name of the calling search space that is used by user phones.
- Step 18** On the Calling Search Space Configuration page, in the Available Partitions list, select the name of the partition created in [Step 5](#) through [Step 7](#). For example, select “VMPilotNumberPT.”  
If the partition that contains the hunt pilot (which is the voice mail pilot number) is not in the calling search space that is used by user phones, the phones are not able to dial the Unity Connection server.
- Step 19** Select the down arrow below the Available Partition list.  
The name of the partition appears in the Selected Partitions list.
- Step 20** Select **Save**.
- Step 21** Repeat [Step 17](#) through [Step 20](#) for each remaining calling search space that needs to access Unity Connection.

## Adding a Device Pool for the Voice Mail Ports

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

*Table 1: Settings for the Device Pool Configuration Page*

Field	Setting
<b>Device Pool Settings</b>	

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

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

## Adding the Voice Mail Ports on Cisco Unified CM

**Step 1** In Cisco Unified CM Administration, expand **Advanced Features > Voice Mail > and select > Cisco Voice Mail Port Wizard**.

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

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

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

The voice mail server name must match the Device Name Prefix field in Unity Connection on the Port Group Basics page for the voice messaging ports, with -VI appended to the end of the name. For example, if the Device Name Prefix in Cisco Unified CM is CiscoUM, the voice mail server name in Unity Connection should be CiscoUM-VI.

**Step 4** Select **Next**.

**Step 5** On the Cisco Voice Mail Ports page, select the number of voice mail ports that you want to add (it should not be more voice mail ports than the Unity Connection licenses enable), then select **Next**.

For a Unity Connection cluster, first enter the number of voice mail ports for the publisher and then for the subscriber, selecting the appropriate server for each creation process.

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

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

**Table 2: Settings for the Cisco Voice Mail Device Information Page**

Field	Setting
Description	Enter <b>Cisco Voice Mail Port</b> or another description for the voice mail device.
Device Pool	Select the name of the device pool you created for the voice mail ports. For example, select Unity Connection Voice Mail Ports.
Calling Search Space	Select the name of a calling search space that allows calls to the user phones and any required network devices.  This calling search space must include partitions that contain all devices Cisco Unity Connection needs to access (for example, during call transfers, message notifications, and MWI activations).
AAR Calling Search Space	Accept the default of <b>None</b> .
Location	Select <b>Hub_None</b> .
Device Security Mode	Select the security mode that you want to use for the voice mail ports. For details on the settings for Cisco Unified CM authentication and encryption of the voice mail ports, see <a href="#">Introduction</a> .
Use Trusted Relay Point	Accept the default setting, or select another setting.

**Step 7** Select **Next**.

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

**Table 3: Settings for the Cisco Voice Mail Directory Numbers Page**

Field	Setting
Beginning Directory Number	Enter the extension number of the first voice mail port.
Partition	Select the name of the partition that you set up for all voice mail port directory numbers. For example, select “VMRestrictedPT.”
Calling Search Space	Select the name of a calling search space that you set up to contain the partition with all voice mail port directory numbers, as set in <a href="#">Step 9</a> of the “ <a href="#">Adding Partitions and a Calling Search Space for Voice Mail Ports</a> ” procedure on page 3-3. For example, select “VMRestrictedCSS.”  Because this calling search space is not used by user phones, users are not able to dial the voice mail ports. However, users can dial the voice mail pilot number.

Field	Setting
AAR Group	Select the automated alternate routing (AAR) group for the voice mail ports. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If you select <b>None</b> , no rerouting of blocked calls attempted.
Internal Caller ID Display	Accept the default of <b>VoiceMail</b> . This text appears on the phone when the pilot number is dialed.
Internal Caller ID Display (ASCII Format)	Accept the default of <b>VoiceMail</b> . This text appears on the phone when the pilot number is dialed.
External Number Mask	Leave this field blank, or specify the mask used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information, and enter <b>X</b> for each digit in the directory number of the device.

**Step 9** Select **Next**.

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

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

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

## Adding the Answering Voice Mail Ports to a Line Group

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

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

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

For a Unity Connection cluster, the line group contains directory numbers for voice mail ports that answer calls on all servers in the Unity Connection cluster. Directory numbers for voice mail ports that only dial out (for example, to set MWIs) on all servers in the Unity Connection cluster must not be included in this line group.

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

Table 4: Settings for the Line Group Configuration Page for Answering Ports

Field	Setting
Line Group Name	Enter <b>Unity Connection Answering Ports</b> or another unique name for line groups.
RNA Reversion Timeout	Accept the default of <b>10</b> .
Distribution Algorithm	<i>(Without a Unity Connection cluster)</i> Select <b>Longest Idle Time</b> . <i>(With a Unity Connection cluster configured)</i> Select <b>Top Down</b> .
No Answer	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .
Busy	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .
Not Available	Accept the default of <b>Try Next Member; Then, Try Next Group in Hunt List</b> .

- Step 4** Under Line Group Member Information, in the Partition list, select the name of the partition that you set up for all voice mail port directory numbers. For example, select “VMRestrictedPT.”
- Step 5** Select **Find**.
- Step 6** In the Available DN/Route Partition list, select the first directory number of a voice mail port that answer calls, and select **Add to Line Group**.
- The directory numbers in the Selected DN/Route Partition list must appear in numerical sequence with the lowest number on top. Otherwise, the integration does not function correctly.
- Step 7** Repeat [Step 6](#) for all remaining directory numbers of voice mail ports that answers calls.
- Do not include directory numbers of voice mail ports that only dial out (for example, to set MWIs). Otherwise, the integration does not function correctly.
- Step 8** Select **Save**.

---

## Adding the Line Group to a Hunt List

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

Table 5: Settings for the Hunt List Configuration Page for Answering Ports

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

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

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

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

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

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

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

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

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

## Adding the Hunt List to a Hunt Pilot Number

**Step 1** In Cisco Unified CM Administration, expand **Call Routing** > **Route/Hunt** > and select > **Hunt Pilot**.

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

**Step 3** On the Hunt Pilot Configuration page, enter the following settings for the hunt pilot.

Table 6: Settings for Hunt Pilot Configuration Page

Field	Setting
Hunt Pilot	Enter the hunt pilot number for the voice mail ports. The hunt pilot number must be different from the extension numbers of the voice mail ports.  The hunt pilot number is the extension number that users enter to listen to their voice messages.

Field	Setting
Route Partition	Select the name of the partition that you set up for the voice mail pilot number. For example, select “VMPilotNumberPT.”
Description	Enter <b>Unity Connection Hunt Pilot</b> or another description.
Numbering Plan	Accept the default setting, or select the numbering plan that you have set up for your system.
Route Filter	Select <b>None</b> , or select the name of the route filter that you set up for your system.
MLPP Precedence	Accept the default setting, or select another setting.
Hunt List	Select the hunt list of voice mail ports that answer calls, which you set up in the <a href="#">Adding the Line Group to a Hunt List</a> .
Route Option	Select <b>Route This Pattern</b> .
Provide Outside Dial Tone	Uncheck the check box.

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

## Specifying the MWI Directory Numbers

**Step 1** In Cisco Unified CM Administration, expand **Advanced Features > Voice Mail > and select > Message Waiting**.

**Step 2** On the Find and List Message Waiting Numbers page, select **Add New**.

**Step 3** On the Message Waiting Configuration page, enter the following settings for turning MWIs on.

*Table 7: Settings for Turning MWIs On*

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

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

**Step 5** Select **Add New**.

**Step 6** Enter the following settings for turning MWIs off.

**Table 8: Settings for Turning MWIs Off**

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

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

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

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

**Step 1** In Cisco Unified CM Administration, expand **Advanced Features > Voice Mail > and 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 9: Settings for the Voice Mail Pilot Configuration Page**

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users dial to listen to their voice messages. This number must be the same as the hunt pilot number that you entered when adding voice mail ports earlier.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition you set up for the voice mail pilot number.
Description	Enter <b>Cisco Unity Connection Pilot</b> or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.



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

## Setting Up the Voice Mail Profile

**Step 1** In Cisco Unified CM Administration, expand **Advanced Features** > **Voice Mail** > **and 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 10: Settings for the Voice Mail Profile Configuration Page*

Field	Setting
Voice Mail Profile Name	Enter a name to identify the voice mail profile.
Description	Enter <b>Unity Connection Profile</b> or another description.
Voice Mail Pilot	Select one of the following: <ul style="list-style-type: none"> <li>The applicable voice mail pilot number that you defined on the Voice Mail Pilot Configuration page</li> <li><b>Use Default</b></li> </ul>
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank.  When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default.  When this check box is checked, this voice mail profile replaces the current default voice mail profile.

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

## Setting Up the Voice Mail Server Service Parameters

**Step 1** In Cisco Unified CM Administration, select **System** > **and then select** > **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 voice mail extensions into directory numbers when turning on or off an MWI.
- Step 6** If you changed any settings, select **Save**. Otherwise, skip the remaining steps in this procedure.
- Step 7** In the Navigation drop-down box, select **Cisco Unified Serviceability** and select **Go**.
- Step 8** In Cisco Unified Serviceability, on the Tools menu, select **Control Center - Feature Services**.
- Step 9** Under CM Services, select **Cisco CallManager** and select **Restart**.

## Creating a New Integration with Cisco Unified CM

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

- Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.
- Step 2** On the Search Phone Systems page, under Display Name, select the name of the default phone system.
- Step 3** On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.
- Step 4** 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 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 5** Select **Save**.
- Step 6** On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.
- Step 7** On the New Port Group page, enter the following settings and select **Save**.

**Table 11: Settings for the New Port Group Page**

Field	Setting
Phone System	Select the name of the phone system that you entered in <a href="#">Step 3</a> .
Create From	Select <b>Port Group Template</b> and select <b>SCCP</b> in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Device Name Prefix	Enter the prefix that Cisco Unified CM adds to the device name for voice ports. This prefix must match the prefix used by Cisco Unified CM.
MWI On Extension	Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs on.

Field	Setting
MWI Off Extension	Enter the extension that you specified in Cisco Unified CM Administration for turning MWIs off.
IPv4 Address or Host Name	<p>Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with 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> <p>If you use Cisco Unified CM authentication and encryption, enter an IP address or host name in this field. The CTL file used for encryption between Unity Connection and Cisco Unified CM requires an IPv4 address or host name, even if you are otherwise using IPv6 addressing.</p>
IPv6 Address or Host Name	<p>Enter the IPv6 address (or host name) of the primary Cisco Unified CM server that you are integrating with 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 IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.</p> <p>The IPv6 address should be in canonical textual representation formats proposed by Internet Engineering Task Force in RFC5952 standard for rendering IPv6 addresses in text. For more details on IPv6 formats, please refer the link <a href="https://tools.ietf.org/html/rfc5952#section-4">https://tools.ietf.org/html/rfc5952#section-4</a></p> <p><b>Note</b> IPv6 is supported in Cisco Unified CM 7.1(2) and later.</p>
IP Address or Host Name	Enter the IP address (or host name) of the primary Cisco Unified CM server that you are integrating with Unity Connection.
Port	Enter the TCP port of the primary Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the primary Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.

**Step 8** On the Port Group Basics page, in the Related Links drop-down box, select **Add Ports** and select **Go**.

**Step 9** On the New Port page, enter the following settings and select **Save**.

Table 12: Settings for the New Port Page

Field	Setting
Enabled	Check this check box.
Number of Ports	Enter the number of voice messaging ports that you want to create in this port group.  <b>Note</b> For a Unity Connection cluster, you must enter the total number of voice messaging ports that is used by all Unity Connection servers. Later, each port is assigned to a specific Unity Connection server.
Phone System	Select the name of the phone system that you entered in <a href="#">Step 3</a> .
Port Group	Select the name of the port group that you added in <a href="#">Step 7</a> .
Server	Select the name Unity Connection server.
Security Mode	Select the Cisco Unified CM security mode that you want to use for the voice messaging ports.

**Step 10** 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 11** 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 13: 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 Unity Connection clusters only)</i> Select the name of the Unity Connection server that you want to handle this port. For details, see <a href="#">Planning the Port Setup</a>
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.

Field	Considerations
Perform Message Notification	Check this check box to designate the port for notifying users of messages. Assign Perform Message Notification to the least busy ports.
Send MWI Requests	Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports.
Allow TRAP Connections	Check this check box so that users can use the port for recording and playback through the phone in Unity Connection web applications. Assign Allow TRAP Connections to the least busy ports.
Outgoing Hunt Order	Enter the priority order in which Unity Connection use the ports when dialing out (for example, if the Perform Message Notification, Send MWI Requests, or Allow TRAP Connections check box is checked). The highest numbers are used first. However, when multiple ports have the same Outgoing Hunt Order number, Unity Connection use the port that has been idle the longest.

Field	Considerations
Security Mode	<p>Select the applicable security mode:</p> <ul style="list-style-type: none"> <li>• <b>Non-secure</b>—The integrity and privacy of call-signaling messages is not ensured because call-signaling messages are sent as clear (unencrypted) text and connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream is not encrypted.</li> <li>• <b>Authenticated</b>—The integrity of call-signaling messages is ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages is not ensured because they are sent as clear (unencrypted) text. In addition, the media stream is not encrypted.</li> <li>• <b>Encrypted</b>—The integrity and privacy of call-signaling messages is ensured on this port because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream is encrypted.</li> </ul> <p><b>Caution</b> The Security Mode setting for Unity Connection voice messaging ports must match the security mode setting for the Cisco Unified CM ports. Otherwise, Cisco Unified CM authentication and encryption fail.</p> <p>The Unity Connection system clock must be synchronized with the Cisco Unified CM system clock for Cisco Unified CM authentication to function immediately. Otherwise, Cisco Unified CM reject the Unity Connection voice messaging ports until the Cisco Unified CM system clock has passed the time stamp in the Unity Connection device certificates.</p> <p><b>Note</b> For requirements and additional information about authentication and encryption with Cisco Unified CM and Unity Connection, see <a href="#">Introduction</a></p>

**Step 12** Select **Save**.

**Step 13** Select **Next**.

- Step 14** Repeat [Step 11](#) through [Step 13](#) for all remaining voice messaging ports for the phone system.
- Step 15** If Cisco Unity Connection does not connect to an AXL server, skip to [Step 28](#). Otherwise, expand **Telephony Integrations**, then select **Phone System**.
- Step 16** On the Search Phone Systems page, select the display name of the phone system that you created in [Step 3](#).
- Step 17** On the Phone System Basics page, in the Edit menu, select **Cisco Unified Communications Manager AXL Servers**.

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

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

- Step 18** On the Edit AXL Servers page, under AXL Servers, select **Add New**.
- Step 19** Enter the following settings for the AXL server and select **Save**.

**Table 14: Settings for the AXL Servers**

Field	Setting
Order	Enter the order of priority for the AXL server. The lowest number is the primary AXL server, the higher numbers are the secondary servers.
IP Address	Enter the IP address of the AXL server.
Port	Enter the AXL server port that Unity Connection connects to. This setting must match the port that the AXL server uses.

- Step 20** Repeat [Step 18](#) and [Step 19](#) for all remaining AXL servers.
- Step 21** Under AXL Server Settings, enter the following settings and select **Save**.

**Table 15: Settings for the AXL Server Settings**

Field	Setting
Username	Enter the username that Unity Connection uses to sign in to the AXL server.  <b>Note</b> This user must match the user name of a Cisco Unified CM application user who is assigned to the “Standard AXL API Access” role.
Password	Enter the password for the user that Unity Connection uses to sign in to the AXL server.  <b>Note</b> This password must match the password of the Cisco Unified CM application user entered in the User Name field.

Field	Setting
Cisco Unified Communications Manager Version	<p>Select the applicable setting that accurately describes the following:</p> <ul style="list-style-type: none"> <li>• The version of Cisco Unified CM that you are integrating with Unity Connection.</li> <li>• Whether the AXL port is enabled for SSL.</li> </ul> <p>If you select the non-SSL version, the AXL port must be a non-SSL port (typically port 80). If you select the SSL-enabled version, the AXL port must be an SSL-enabled port (typically port 443 or port 8443).</p>
Enable End User PIN Synchronization for Primary AXL Server	<p>Check this check box to enable PIN synchronization between Unity Connection and Cisco Unified CM for the users having same user ID (alias in Unity Connection).</p> <p>After enabling the feature whenever user updates the PIN on Cisco Unity Connection, the PIN gets synchronized with Cisco Unified CM and vice-versa.</p> <p>Default setting: Check box is not checked.</p> <p>For more information on PIN Synchronization, see the "PIN Synchronization between Unity Connection and Cisco Unified CM" section of the "User Settings" chapter of the <i>System Administration Guide for Cisco Unity Connection Release 12.x</i> available at <a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12/administration/guide/b_12ucosagx.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12/administration/guide/b_12ucosagx.html</a>.</p>
Ignore Certificate Errors	<p>Check the check box to ignore certificate validation errors for AXL Servers. When the check box is unchecked, Unity Connection validates the certificate for the AXL servers. However, before checking the checkbox make sure that the tomcat root certificate of Cisco Unified CM must be uploaded to tomcat trust of Unity Connection server.</p> <p>Default setting: Check box is checked.</p> <p>For more information on certificates, see "Security" chapter of Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14 at <a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14ucosagx.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14ucosagx.html</a>.</p>

**Step 22** To add a corresponding application server to Cisco Unified CM, sign in to Cisco Unified CM Administration.

**Step 23** In Cisco Unified CM Administration, navigate to System > Application Server page.

**Step 24** On the Find and List Application Servers page, select **Find** to display all application servers.

**Step 25** In the Name column, select the name of the Cisco Unity Connection server.



**Step 26** On the Application Server Configuration page, in the Available Application User field, select the Cisco Unified CM application user that you used in [Step 21](#) and select the **down arrow** to move it to the Selected Application User field.

**Step 27** Select Save.

**Step 28** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Port Group**.

**Step 29** On the Search Port Groups page, select the display name of the port group that you created with the phone system integration in [Step 7](#).

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

**Step 30** On the Port Group Basics page, on the Edit menu, select **Servers**.

**Step 31** On the Edit Servers page, do the following substeps if the Cisco Unified CM cluster has secondary servers. Otherwise, skip to [Step 32](#).

- a) Under Cisco Unified Communications Manager Servers, select **Add**.
- b) Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

**Table 16: Settings for the Cisco Unified Communications Manager 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	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	Enter the IPv6 address (or host name) of the secondary Cisco Unified CM server.  You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.  <b>Note</b> IPv6 is supported in Cisco Unified CM 7.1(2) and later.
IP Address or Host Name	Enter the IP address (or host name) of the secondary Cisco Unified CM server.
Port	Enter the TCP port of the Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.

Field	Setting
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.
Server Type	Select <b>Cisco Unified Communications Manager</b> .

- c) Repeat [Step 31](#) for all remaining Cisco Unified CM servers in the cluster.

**Step 32**

Do the following substeps if the Cisco Unified CM cluster uses authentication or encryption for the voice messaging ports.

- Under TFTP Servers, select **Add**.
- Enter the following settings for the TFTP server and select **Save**.

**Table 17: Settings for the TFTP Server**

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	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	Enter the IPv6 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.  <b>Note</b> IPv6 is supported in Cisco Unified CM 7.1(2) and later.
IP Address or Host Name	Enter the IP address (or host name) of the TFTP server.

- c) Repeat [Step 32](#) for all remaining TFTP servers in the Cisco Unified CM cluster.

**Step 33**

If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**. Otherwise, skip to [Step 37](#).

**Step 34**

On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.

**Step 35**

On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

**Table 18: 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 connects to.
Trunk Access Code	Enter the extra digits that Unity Connection must dial to transfer calls through the gateway to extensions on the previously existing phone system.

**Step 36** Repeat [Step 34](#) and [Step 35](#) for all remaining phone system trunks that you want to create.

**Step 37** 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 38** In the Task Execution Results window, select **Close**.

---





## CHAPTER 4

# Configuring Voice Messaging Ports Configuration for a Unity Connection Cluster

- [Configuring Voice Messaging Ports Configuration for a Unity Connection Cluster](#), on page 31

## Configuring Voice Messaging Ports Configuration for a Unity Connection Cluster

### Introduction

This chapter provides information for configuring voice messaging ports for a Unity Connection cluster.

The Cisco Unity Connection cluster feature provides high availability Unity Connection voice messaging through two Unity Connection servers.

For details on the Unity Connection cluster feature, see the [Configuring Cisco Unity Connection Cluster](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html) chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 14 available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/install\\_upgrade/guide/b\\_14cuciumg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html).

### Voice Messaging Port for Unity Connection Cluster

For a Unity Connection cluster, you must know how the voice messaging ports function—which ports answer calls and which ports dial out (for setting MWIs and for sending message notifications). Depending on the function of the ports, you assign them to the applicable server in the Unity Connection cluster:

Answering ports	Beginning with the answering port that has the lowest number in its display name, assign half the answering ports to the subscriber server so that the subscriber server answer most incoming calls. Assign the remaining answering ports to the publisher server.
Dial-out ports (for MWIs and notifications)	Beginning with the dial-out port that has the lowest number in its display name, assign half the dial-out ports to the primary server so that the primary server handle MWIs and notification calls. Assign the remaining dial-out ports to the subscriber server.

For example, an eight-port system with six answering ports and two dial-out ports can be configured as follows.

Port Function	Port Display Name	Server
Answering	UCM1-001	Subscriber
	UCM1-002	Subscriber
	UCM1-003	Subscriber
	UCM1-004	Publisher
	UCM1-005	Publisher
	UCM1-006	Publisher
Dialing out	UCM1-007	Publisher
	UCM1-008	Subscriber

Under normal conditions, the Unity Connection cluster handles calls in the following manner:

- The subscriber server answer most incoming calls. If no answering ports on the subscriber server are available, the publisher server answer calls.
- The publisher server dial out for MWIs and notifications. If no dial-out ports on the publisher server are available, the subscriber server dial out for MWIs and notifications.

## Voice Messaging Ports Configuration for a Unity Connection Cluster

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	In Cisco Unity Connection Administration, expand <b>Telephony Integrations</b> and select <b>Port</b> .	
<b>Step 2</b>	On the Search Ports page, select the display name of the first voice messaging port in the Unity Connection cluster.	<b>Caution</b> All ports for all Unity Connection servers must appear on the Search Ports page. Otherwise, the Unity Connection cluster has not been correctly configured and does not function correctly.
<b>Step 3</b>	On the Port Basics page, in the Server field, select the name of the applicable Unity Connection server depending on the port function. For details, see the <a href="#">Voice Messaging Port for Unity Connection Cluster</a> .	
<b>Step 4</b>	Select <b>Save</b> .	
<b>Step 5</b>	Select <b>Next</b> .	
<b>Step 6</b>	Repeat Step 3 through Step 5 for all remaining voice messaging ports in the Unity Connection cluster.	



## CHAPTER 5

# Testing the Integration

To test whether Cisco Unity Connection and the phone system are integrated correctly, do the following procedures:

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

- The "[Installing Cisco Unity Connection](#)" chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection*, Release 14, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/install\\_upgrade/guide/b\\_14cuciumg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html).
- *Troubleshooting Guide for Cisco Unity Connection Release 14*, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/troubleshooting/guide/b\\_14cuctsg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/troubleshooting/guide/b_14cuctsg.html).
- [Testing the Telephony Integration](#), on page 33
- [Setting Up the Test Configuration](#), on page 34
- [Testing an External Call with Release Transfer](#), on page 35
- [Testing Listening to Messages](#), on page 35
- [Setting Up Supervised Transfer on Cisco Unity Connection](#), on page 36
- [Testing Supervised Transfer](#), on page 36
- [Deleting the Test User](#), on page 36
- [Testing Cisco Unified CM Authentication and Encryption](#), on page 37

## Testing the Telephony Integration

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Go to Telephony Integrations and select Phone System on Cisco Unity Connection Administration.	
<b>Step 2</b>	Select the Phone System from the list for which configuration needs to be tested.	
<b>Step 3</b>	In the Related Links drop-down list, select <b>Check Telephony Configuration</b> and select <b>Go</b> 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.
<b>Step 4</b>	In the Task Execution Results window, select <b>Close</b> .	

# Setting Up the Test Configuration

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

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

- Step 3** In Cisco Unity Connection Administration, expand **Users** and 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, click **Message Waiting Indicators**.
- Step 9** On the Message Waiting Indicators page, click the message waiting indicator. If no message waiting indication is in the table, click **Add New**.
- Step 10** On the Edit Message Waiting Indicator page, enter the following settings.

*Table 19: 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** and select **Save**.
- Step 16** Minimize the Cisco Unity Connection Administration window.
- Do not close the Cisco Unity Connection Administration window because you use it again in a later procedure.
- Step 17** Sign in to the Real-Time Monitoring Tool (RTMT).
- Step 18** On the Unity Connection menu, select **Port Monitor**. The Port Monitor tool appears in the right pane.
- Step 19** In the right pane, select **Start Polling**. The Port Monitor display which port is handling the calls that you make.



## Testing an External Call with Release Transfer

---

- Step 1** From Phone 2, enter the access code necessary to get an outside line, and then enter the number outside callers use to dial directly to 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 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 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 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 Unity Connection are successfully integrated for turning on MWIs.
- 

## Testing Listening to Messages

---

- Step 1** From Phone 1, enter the internal pilot number for 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 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 hear the extension number for Phone 1). Hearing the recorded name means that 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 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.
-

## Setting Up Supervised Transfer on Cisco Unity Connection

---

- Step 1** In Cisco Unity Connection Administration, on the Edit Transfer Option page of 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 Unity Connection Administration window because you use it again in a later procedure.
- 

## Testing Supervised Transfer

---

- Step 1** From Phone 2, enter the access code necessary to get an outside line, and then enter the number outside callers use to dial directly to 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 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 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** and exit RTMT.
- 

## Deleting the Test User

---

- Step 1** In Cisco Unity Connection Administration, expand **Users** and 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**.
-

# Testing Cisco Unified CM Authentication and Encryption

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

- 
- 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.
- 

If any of the above steps indicate a failure, see the following documentation as applicable:

- The “[Installing Cisco Unity Connection](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html)” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 14, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/install\\_upgrade/guide/b\\_14cuciumg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html).
- Troubleshooting Guide for Cisco Unity Connection *Release 14*, available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/14/troubleshooting/guide/b\\_14cuctsg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/troubleshooting/guide/b_14cuctsg.html).





## CHAPTER 6

# Changing the Number of Voice Messaging Ports

- [Changing the Number of Voice Messaging Ports, on page 39](#)

## Changing the Number of Voice Messaging Ports

### Introduction

To change the number of voice messaging ports in Cisco Unified Communications Manager and in Cisco Unity Connection for an existing integration, use Cisco Voice Mail Port Wizard.

See the following:

- To add voice mail ports in Cisco Unified CM Administration through the Cisco Voice Mail Port Wizard, see the [Adding Voice Messaging Ports](#) procedure in the chapter for the applicable version of Cisco Unified CM.
- To remove voice mail ports in Cisco Unified CM Administration through the Cisco Voice Mail Port Wizard, see the Help on Cisco Unified CM Administration.

### Adding Voice Messaging Ports

The following task list describes the process for Adding Voice Messaging Ports in Cisco Unity Connection Administration

---

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations** and select **Port**.

**Note** The maximum number of voice messaging ports that can be added in Unity Connection depends on the OVA template of the virtual machine.

**Step 2** On the Search Ports page, under Port Search Results, select **Add New**.

**Step 3** On the New Port page, enter the applicable settings and select **Save**.

Make sure that there are an appropriate number of ports set to answer calls and an appropriate number of ports set to dial out. Otherwise, the integration does not function correctly. For details, see to the "[Planning the Voice Messaging Ports](#)" chapter.

**Step 4** If you are not using Cisco Unified CM authentication and encryption, skip to [Step 10](#).

If you are using Cisco Unified CM authentication and encryption, in Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, and then select **Root Certificate**.

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

**Step 5** On the View Root Certificate page, **Right-select to Save the Certificate as a File** link, and select **Save Target As**.

**Step 6** In the Save As dialog box, browse to the location where you want to save the Unity Connection root certificate as a file.

**Step 7** For Cisco Unified CM 5.x and later, in the File Name field, confirm that the extension is .pem (rather than .htm), and select **Save**.

**Step 8** In the Download Complete dialog box, select **Close**.

**Step 9** Upload the Unity Connection root certificate to all Cisco Unified CM servers in this Cisco Unified CM phone system integration by doing the following substeps.

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

- a) On the Cisco Unified CM server, sign in to Cisco Unified Operating System Administration.
- b) In Cisco Unified Operating System Administration, on the Security menu, select **Certificate Management**.
- c) On the Certificate List page, select **Upload Certificate**.
- d) On the Upload Certificate page, in the Certificate Name drop-down box, select **CallManager-trust**.
- e) In the Root Certificate field, enter **Cisco Unity Connection Root Certificate**.
- f) To the right of the Upload File field, select **Browse**.
- g) In the Choose File dialog box, browse to the Cisco Unity Connection root certificate that you saved in [Step 7](#).
- h) Follow the on-screen instructions.
- i) Repeat [Step 9a](#). through [Step 9h](#). on all remaining Cisco Unified CM servers in the Cisco Unified CM cluster.
- j) In Cisco Unity Connection Administration, in the Related Links drop-down list, select **Check Telephony Configuration** and select **Go** to confirm the Unity Connection to the Cisco Unified CM servers.

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

k) In the Task Results window, select **Close**.

**Step 10** Sign out of Cisco Unity Connection Administration.

## Deleting Voice Messaging Ports

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > and select > Port**.

**Step 2** In the Search Port page, under Port Search Results, check the check boxes next to the voice messaging ports that you want to delete.

**Step 3** Select **Delete Selected**.

**Step 4** For the remaining voice messaging ports in the port group, change the settings as necessary so that there are an appropriate number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out.

**Step 5** In Cisco Unity Connection Administration, 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 Unity Connection again.

**Step 6** In the Task Execution Results window, select **Close** and sign out of Cisco Unity Connection Administration.

---







## CHAPTER 7

# Cisco Unified Communications Manager Authentication and Encryption

---

- [Cisco Unified Communications Manager Authentication and Encryption, on page 43](#)

## Cisco Unified Communications Manager Authentication and Encryption

### Introduction

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

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

### Cisco Unified CM Security Features

Cisco Unified CM can secure the connection with Unity Connection against these threats. The Cisco Unified CM security features are used by Unity Connection as described in Table 7.

## Cisco Unified CM Security Features Used by Unity Connection

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

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





## CHAPTER 8

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

---

- [Adding Cisco Unified Communications Manager Express to a Cisco Unified Communications Manager Integration, on page 47](#)

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

### Overview

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

There are the following considerations:

- The version of Cisco Unified CM Express and the version of the Unity Connection must be a supported combination in the Compatibility Matrix for Cisco Unity Connection at <http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html>.
- The Cisco Unified CM phone system integration is created before adding the Cisco Unified CM Express server.

### Adding Cisco Unified CM Express Server to Cisco Unified CM Phone System Integration

---

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

## 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 IP 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 enter any value in this field as IPv6 is not supported for Cisco Unified CM Express phone system integrations.
Port	Enter the TCP port of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM Express server that you are adding to the Cisco Unified CM port group. We recommend that you use the default setting.
Server Type	Select <b>Cisco Unified Communications Manager Express</b> .

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

**Step 7** On the Edit menu, select **Advanced Settings**.

**Step 8** On the Edit Advanced Settings page, in the Delay After Answer field, enter **1000** and select **Save**.

**Step 9** On the Edit menu, select **Port Group Basics**.

**Step 10** On the Port Group Basics page, 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 11** When prompted that the test 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 Unity Connection again.

**Step 12** In the Task Execution Results window, select **Close** and sign out of Cisco Unity Connection Administration.

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

When a Cisco Unified Survivable Remote Site Telephony (SRST) router is a 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 Unity Connection to a branch office fails.
- **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 do 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 fail.

When the Cisco Unified SRST router uses PRI/BRI connections, the caller ID for calls from a branch office to Unity Connection may be the full number (exchange plus extension) provided by the PSTN and therefore may not match the extension of the Unity Connection user. If this is the case, you can let Unity Connection recognize the caller ID with 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](http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html).

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

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

AAR can route calls over the PSTN when the WAN is oversubscribed. However, when calls are rerouted over the PSTN, RDNIS can be affected. Incorrect RDNIS information can affect voice mail calls that are rerouted over the PSTN by AAR when Cisco Unity Connection is remote from its messaging clients. If the RDNIS information is not correct, the call do not reach the voice mail box of the dialed user, 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.







## INDEX

### P

ports [3](#), [4](#), [39](#)

changing the number [39](#)

planning how many will answer calls [4](#)

planning how many will dial out [4](#)

planning number to install [3](#)

ports (*continued*)

planning setup [3](#)

### V

voice messaging ports, changing the number [39](#)

