# System Administration Guide for Cisco Unity Connection

Release 10.x
November 2013

**Cisco Systems, Inc.**
www.cisco.com

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

Text Part Number:

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

*System Administration Guide for Cisco Unity Connection Release 10.x*

© 2013 Cisco Systems, Inc. All rights reserved.

**Preface** xix

Audience and Use xix

Documentation Conventions xix

Cisco Unity Connection Documentation xx

Documentation References to Cisco Unified Communications Manager Business Edition (CMBE) xx

Obtaining Documentation and Submitting a Service Request xxi

Cisco Product Security Overview xxi

CHAPTER 1 **Configuring the Browser on a Cisco Unity Connection 10.x Administrator Workstation** 1-1

Configuring Firefox on a Cisco Unity Connection 10.x Administrator Workstation 1-1

Configuring Microsoft Internet Explorer on a Cisco Unity Connection 10.x Administrator Workstation 1-2

CHAPTER 2 **Accessing and Using Cisco Unity Connection Administration 10.x** 2-1

Accessing and Exiting Cisco Unity Connection Administration 10.x 2-1

Cisco Unity Connection Administration 10.x User Interface 2-2

Using Cisco Unity Connection Administration 10.x Help 2-3

Finding Records in Cisco Unity Connection Administration 10.x 2-3

Accessing Other Cisco Unity Connection Administration 10.x Locations in the Network 2-4

CHAPTER 3 **Administrative Tools in Cisco Unity Connection 10.x** 3-1

Application Plug-ins in Cisco Unity Connection 10.x 3-2

Cisco Unified Backup and Restore Application Suite (COBRAS) in Cisco Unity Connection 10.x 3-2

Cisco Unity Connection Administration 10.x 3-2

Cisco Unity Connection 10.x Bulk Administration Tool 3-3

Cisco Unity Connection 10.x Custom Keypad Mapping Tool 3-3

Cisco Unity Connection 10.x Grammar Statistics Tool 3-4

Cisco Unity Connection 10.x Import and Synch Users Tools 3-4

Cisco Unity Connection 10.x Migrate Messages Utility 3-5

Cisco Unity Connection 10.x Migrate Users Utility 3-5

Cisco Unity Connection Serviceability 10.x 3-6

Cisco Unity Connection 10.x Show Dependency Results 3-6

Cisco Unity Connection 10.x Task Management Tool 3-6
Disaster Recovery System in Cisco Unity Connection 10.x 3-7
Cisco Voice Technology Group Subscription Tool in Cisco Unity Connection 10.x 3-7
Real-Time Monitoring Tool in Cisco Unity Connection 10.x 3-7
Cisco Unified Serviceability in Cisco Unity Connection 10.x 3-8
Remote Database Administration Tools in Cisco Unity Connection 10.x 3-8
Enabling Database Access for Remote Administration Tools 3-9
Cisco Utilities Database Link for Informix (CUDLI) in Cisco Unity Connection 10.x 3-9
Unity Connection User Data Dump (CUDD) in Cisco Unity Connection 10.x 3-10
Wallet Card Wizard in Cisco Unity Connection 10.x 3-10

CHAPTER 4 **Call Management Overview in Cisco Unity Connection 10.x 4-1**
Overview of Call Management Concepts in Cisco Unity Connection 10.x 4-1
Call Handlers in Cisco Unity Connection 10.x 4-2
Directory Handlers in Cisco Unity Connection 10.x 4-3
Interview Handlers in Cisco Unity Connection 10.x 4-3
Call Routing Tables in Cisco Unity Connection 10.x 4-4
How Call Routing Rules Work 4-4
Using Routing Rules with the Route from Next Call Routing Rule Action 4-6
Restriction Tables in Cisco Unity Connection 10.x 4-6
How Restriction Tables Work 4-7
Schedules and Holidays in Cisco Unity Connection 10.x 4-8
Default Cisco Unity Connection 10.x Automated Attendant Behavior 4-9

CHAPTER 5 **Creating a Call Management Plan in Cisco Unity Connection 10.x 5-1**
Creating a Call Management Map in Cisco Unity Connection 10.x 5-1
Implementing a Call Management Plan in Cisco Unity Connection 10.x 5-2

CHAPTER 6 **Managing Call Handlers in Cisco Unity Connection 10.x 6-1**
Overview of Default Call Handlers in Cisco Unity Connection 10.x 6-1
Creating, Modifying, and Deleting Call Handler Templates in Cisco Unity Connection 10.x 6-2
Creating Call Handlers in Cisco Unity Connection 10.x 6-4
Modifying Call Handlers in Cisco Unity Connection 10.x 6-5
Overview of Call Handler Greetings in Cisco Unity Connection 10.x 6-6
Managing Call Handler Greetings in Cisco Unity Connection 10.x 6-8
Managing Caller Input During Greetings in Cisco Unity Connection 10.x 6-9

Offering One-Key Dialing During Call Handler Greetings 6-9
Offering System Transfers 6-10
Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter 6-10
Changing Phone Language Settings in Cisco Unity Connection 10.x 6-12
Taking Messages in Cisco Unity Connection 10.x 6-12
Transferring Calls in Cisco Unity Connection 10.x 6-13
Deleting Call Handlers in Cisco Unity Connection 10.x 6-13

CHAPTER 7 **Managing Directory Handlers in Cisco Unity Connection 10.x** 7-1
Overview of the Default Directory Handler in Cisco Unity Connection 10.x 7-1
Creating a Directory Handler in Cisco Unity Connection 10.x 7-2
Modifying a Directory Handler in Cisco Unity Connection 10.x 7-2
Changing Phone Language Settings in Cisco Unity Connection 10.x 7-3
Routing Calls to a Voice Directory Handler in Cisco Unity Connection 10.x 7-4
Deleting a Directory Handler in Cisco Unity Connection 10.x 7-5

CHAPTER 8 **Managing Interview Handlers in Cisco Unity Connection 10.x** 8-1
Creating Interview Handlers in Cisco Unity Connection 10.x 8-1
Modifying Interview Handlers in Cisco Unity Connection 10.x 8-2
Changing Phone Language Settings in Cisco Unity Connection 10.x 8-3
Deleting Interview Handlers in Cisco Unity Connection 10.x 8-4

CHAPTER 9 **Managing Custom Recordings in Cisco Unity Connection 10.x** 9-1
Overview of the Custom Recordings in Cisco Unity Connection 10.x 9-1
Adding a New Custom Recording in Cisco Unity Connection 10.x 9-2
Modifying a Custom Recording in Cisco Unity Connection 10.x 9-2
Setting After Message Sent Custom Recording in Cisco Unity Connection 10.x 9-3
Deleting a Custom Recording in Cisco Unity Connection 10.x 9-5

CHAPTER 10 **Managing Call Routing Tables in Cisco Unity Connection 10.x** 10-1
Overview of Default Call Routing Rules in Cisco Unity Connection 10.x 10-1
Adding Call Routing Rules in Cisco Unity Connection 10.x 10-2
Modifying Call Routing Rules in Cisco Unity Connection 10.x 10-2
Changing Phone Language Settings in Cisco Unity Connection 10.x 10-3
Changing the Order of Call Routing Rules in Cisco Unity Connection 10.x 10-3
Deleting Call Routing Rules in Cisco Unity Connection 10.x 10-4

CHAPTER 11 **Managing Video Greetings in Cisco Unity Connection 10.x** 11-1

Overview of Video Greetings in Cisco Unity Connection 11-1

Installing, Integrating, and Accessing Cisco MediaSense 11-3

Installing and Integrating Cisco MediaSense 11-3

Accessing Cisco MediaSense Administration 11-3

Uploading Cisco logo from Cisco MediaSense 11-4

Supported Specifications of a Customized logo 11-4

Disabling Cisco MediaSense Prune Policy 11-4

Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x 11-5

Creating Video Service in Cisco Unity Connection 10.x 11-5

Modifying Video Service in Cisco Unity Connection 10.x 11-6

Creating Video Services Accounts in Cisco Unity Connection 10.x 11-7

Deleting Video Service Account in Cisco Unity Connection 10.x 11-8

Using the Cisco Unity Connection 10.x Bulk Administration Tool to Manage Video Services Accounts 11-8

Pre-checks Required for Video Greetings 11-9

CHAPTER 12 **Managing Schedules and Holidays in Cisco Unity Connection 10.x** 12-1

Overview of Default Schedules in Cisco Unity Connection 10.x 12-1

Designating Holidays in Cisco Unity Connection 10.x 12-1

Creating Schedules in Cisco Unity Connection 10.x 12-2

Modifying Schedules in Cisco Unity Connection 10.x 12-2

Deleting Schedules in Cisco Unity Connection 10.x 12-3

CHAPTER 13 **Managing Restriction Tables in Cisco Unity Connection 10.x** 13-1

Overview of Default Restriction Tables in Cisco Unity Connection 10.x 13-1

Creating Restriction Tables in Cisco Unity Connection 10.x 13-2

Modifying Restriction Tables in Cisco Unity Connection 10.x 13-3

Deleting Restriction Tables in Cisco Unity Connection 10.x 13-3

CHAPTER 14 **Setting Up System Transfers in Cisco Unity Connection 10.x** 14-1

System Transfer Overview in Cisco Unity Connection 10.x 14-1

Task List: Offering Caller System Transfers in Cisco Unity Connection 10.x 14-2

Configuring a Greeting to Allow System Transfers 14-3

Task List: Offering User System Transfers in Cisco Unity Connection 10.x 14-4

CHAPTER 15 **Cisco Unity Connection 10.x Conversation** 15-1

How Outside Callers Interact With Cisco Unity Connection 10.x by Phone 15-1

How Users Interact With Cisco Unity Connection 10.x by Phone 15-1

How Administrators Can Customize the User Conversation in Cisco Unity Connection 10.x 15-2

Advanced Conversation Configuration Settings 15-2

Customizing the Language of System Prompts 15-2

Class of Service Settings 15-3

User Account and Template Settings 15-3

Using the Custom Keypad Mapping Tool 15-5

How Users Can Customize the User Conversation in Cisco Unity Connection 10.x 15-5

CHAPTER 16 **Changing Conversation Settings for All Users in Cisco Unity Connection 10.x** 16-1

Accessibility Settings in Effect During the PIN Entry Conversation in Cisco Unity Connection 10.x 16-2

Addressing Priority Lists in Cisco Unity Connection 10.x 16-2

Addressing and Recording Order in Cisco Unity Connection 10.x 16-3

Announcing to Users When Messages Are Marked Secure 16-4

Announcing When a Message Has Been Sent to Multiple Recipients, and Listing Message Recipients 16-4

Automatically Adding Alternate Extensions in Cisco Unity Connection 10.x 16-4

Call Holding Wait Time in Cisco Unity Connection 10.x 16-5

Announcing Message Status on Reply or Reply-All in Cisco Unity Connection 16-6

Announcing Recipient List on Reply or Reply-All in Cisco Unity Connection 10.x 16-7

Announcing Message Status on Reply or Reply-All in Cisco Unity Connection 16-8

Announcing Recipient List on Reply or Reply-All in Cisco Unity Connection 16-9

Warning users on Reply-All when Number of Recipients Exceeds Maximum in Cisco Unity Connection 16-10

Caller Information in Cisco Unity Connection 10.x 16-10

Dial Prefix Settings for Live Reply to Unidentified Callers in Cisco Unity Connection 10.x 16-11

Deleting Messages in Cisco Unity Connection 10.x 16-12

Language of System Prompts in Cisco Unity Connection 10.x 16-13

Allowing Users to Playback Video Greetings in Cisco Unity Connection 10.x 16-14

Routing Users to the Voice-Recognition or Touchtone Conversation Style 16-16

Signing In to Cisco Unity Connection 10.x from a User Greeting 16-17

Requesting Users Re-Enter Only the PIN After a Failed PIN Entry in Cisco Unity Connection 10.x 16-18

Saving Speed and Volume Changes Made by Users in Cisco Unity Connection 10.x 16-19

Skipping Messages: Saving New Messages in Cisco Unity Connection 10.x 16-19

Voice Recognition: Allowing Users to Say Their Voicemail PINs in Cisco Unity Connection 10.x 16-20
Voice Recognition: Confirmation Confidence Threshold in Cisco Unity Connection 10.x 16-21
Voice Recognition: Global Nickname List in Cisco Unity Connection 10.x 16-22
Additional Advanced Conversation Configuration Settings in Cisco Unity Connection 10.x 16-23

CHAPTER 17 **Custom Keypad Mapping Tool in Cisco Unity Connection 10.x 17-1**
Using the Custom Keypad Mapping Tool in Cisco Unity Connection 10.x 17-1
Guidelines for Assigning Keys to Menu Options 17-2
Setting a Keypad Mapping to Match an Existing Conversation Mapping 17-2
Conversation Menus That Can Be Customized in Cisco Unity Connection 10.x 17-3
Main Menu Tab 17-3
Message Playback Menu Tabs (Message Header Tab, Message Body Tab, and Message Footer Tab) 17-5
After Message Menu Tab 17-9
Settings Menu Tab 17-11
Message Settings Menu Tab 17-12
Preferences Menu Tab 17-12
Documenting Your Keymap in Cisco Unity Connection 10.x 17-13

CHAPTER 18 **Changing the Audio Format of Recordings and Media Streams in Cisco Unity Connection 10.x 18-1**
Changing the Audio Format That Cisco Unity Connection 10.x Uses for Calls 18-1
Changing the Audio Format for Recordings in Cisco Unity Connection 10.x 18-2

CHAPTER 19 **Changing the Video Format of Greetings in Cisco Unity Connection 10.x 19-1**
Changing the Video Format that Cisco Unity Connection 10.x Uses for Calls 19-1
Changing the Video Format for Greetings in Cisco Unity Connection 10.x 19-2

CHAPTER 20 **Managing Recorded Greetings and Recorded Names in Cisco Unity Connection 10.x 20-1**
Using the Media Master to Record Greetings and Names in Cisco Unity Connection 10.x 20-1
Using the 10.x Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings 20-2
Setting Up the 10.x Cisco Unity Greetings Administrator 20-4
Changing the Audio Format for Recording Greetings and Names in Cisco Unity Connection 10.x 20-5

CHAPTER 21 **Specifying Password, PIN, Sign-In, and Lockout Policies in Cisco Unity Connection 10.x 21-1**
Specifying Password, PIN, Sign-In, and Lockout Policies by Using Authentication Rules 21-1
Creating and Modifying Authentication Rules, and Assigning Rules to Users 21-2

CHAPTER 22 **Messaging in Cisco Unity Connection 10.x** 22-1

Types of Messages in Cisco Unity Connection 10.x 22-1

Message Recording in Cisco Unity Connection 10.x 22-5

Configuring the Termination Warning Prompt for the End of Recording 22-6

Default Recipient Accounts in Cisco Unity Connection 10.x 22-7

Dispatch Messages in Cisco Unity Connection 10.x 22-8

Dispatch Messaging Limitations and Behavioral Notes 22-9

Message Delivery in Cisco Unity Connection 10.x 22-10

How Cisco Unity Connection Handles Messages That Cannot Be Delivered 22-11

How Cisco Unity Connection Handles Messages When System Components Are Unavailable 22-11

How Cisco Unity Connection Handles Messages That Are Interrupted by Disconnected Calls 22-12

How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded 22-13

How Cisco Unity Connection Handles Messages When Maximum Mailbox Store Size Is Exceeded 22-14

Message Delivery and Sensitivity Options in Cisco Unity Connection 10.x 22-14

Message Actions in Cisco Unity Connection 10.x 22-16

Message Subject Line Formats in Cisco Unity Connection 10.x 22-17

Subject Line Parameters 22-17

Subject Line Format Examples 22-19

Subject Line Format Configuration 22-19

Message Storage and Disk Capacity in Cisco Unity Connection 10.x 22-20

Deleting Messages in Cisco Unity Connection 10.x 22-20

Soft Deletes and Hard Deletes 22-21

Deleting Messages by Way of Message Aging Policies 22-21

Message File Shredding for Secure Deletes 22-22

Message Access in Cisco Unity Connection 10.x 22-22

Configuring Live Record in Cisco Unity Connection 10.x 22-22

Configuring Access to RSS Feeds of Voice Messages in Cisco Unity Connection 10.x 22-25

Allowing Insecure Connections to RSS Feeds 22-25

Configuring an RSS Reader to View Voice Messages 22-26

RSS Feed Limitations and Behavioral Notes 22-26

CHAPTER 23 **Configuring IMAP Settings in Cisco Unity Connection 10.x** 23-1

Overview of SMTP Message Handling in Cisco Unity Connection 10.x 23-1

Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook 10.x 23-2

Recommendations for Deploying IMAP Access in Cisco Unity Connection 10.x 23-3

Task List for Configuring IMAP Access in Cisco Unity Connection 10.x 23-3

Procedures for Configuring IMAP Access in Cisco Unity Connection 10.x 23-5
Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host 23-5
Configuring Message Relay Settings 23-5
Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication 23-6
Configuring SMTP Message Parameters 23-7

CHAPTER 24 **Configuring Transcription (SpeechView) in Cisco Unity Connection 10.x** 24-1
Overview of SpeechView in Cisco Unity Connection 10.x 24-1
SpeechView Security Considerations 24-3
Recommendations for Deploying SpeechView 24-3
Task List for Configuring SpeechView in Cisco Unity Connection 10.x 24-4
Procedures for Configuring SpeechView in Cisco Unity Connection 10.x 24-5
Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host 24-5
Configuring the Cisco Unity Connection Server to Accept Messages From Your Email System 24-5
Configuring Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server 24-6
Configuring the SpeechView Transcription Service 24-7
SpeechView Reports in Cisco Unity Connection 10.x 24-8

CHAPTER 25 **Managing Mailbox Stores in Cisco Unity Connection 10.x** 25-1
How Multiple Mailbox Stores Work in Cisco Unity Connection 10.x 25-1
Replication 25-2
User Templates 25-2
Maximum Size of a Mailbox Store Before Warnings Are Logged 25-3
Backups with Multiple Mailbox Stores 25-3
Creating a Mailbox Store in Cisco Unity Connection 10.x 25-4
Moving Mailboxes Between Mailbox Stores in Cisco Unity Connection 10.x 25-5
Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged in Cisco Unity Connection 10.x 25-6
Deleting a Mailbox Store in Cisco Unity Connection 10.x 25-6
Disabling and Re-Enabling a Mailbox Store in Cisco Unity Connection 10.x 25-7

CHAPTER 26 **Controlling the Size of Mailboxes in Cisco Unity Connection 10.x** 26-1
Specifying Mailbox Size Quotas in Cisco Unity Connection 10.x 26-1
Managing Mailbox Quota Alert in Cisco Unity Connection 10.x 26-3
Configuring Mailbox Quota Alert Text 26-3
Managing Message Aging Policies in Cisco Unity Connection 10.x 26-4
About Message Aging Alerts 26-6

Adding a Message Aging Policy 26-6
Changing a Message Aging Policy 26-7
Deleting a Message Aging Policy 26-7
Configuring a Smart Host for Message Aging Alerts 26-8
Configuring Message Aging Alert Text 26-8
Configuring Message Aging When Single Inbox Is Configured 26-9
Message Recording Expiration 26-9

CHAPTER 27 **Setting Up HTML, SMTP, and SMS (SMPP) Message Notifications in Cisco Unity Connection 10.x** 27-1
Setting Up HTML or SMTP Message Notifications in Cisco Unity Connection 10.x 27-1
Setting Up SMS (SMPP) Message Notifications in Cisco Unity Connection 10.x 27-2
Task List for Setting Up SMS (SMPP) Message Notifications 27-4

CHAPTER 28 **Configuring SSL in Cisco Unity Connection 10.x** 28-1
Deciding Whether to Create and Install an SSL Certificate in Cisco Unity Connection 10.x 28-1
Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 10.x 28-2
Installing Microsoft Certificate Services (Windows Server 2003 Only) in Cisco Unity Connection 10.x 28-5
Exporting the Issuer Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only) in Cisco Unity Connection 10.x 28-6

CHAPTER 29 **Setting Up Broadcast Messaging in Cisco Unity Connection 10.x** 29-1
How System Broadcast Messages Work in Cisco Unity Connection 10.x 29-1
Task List for Offering Broadcast Messaging to Users in Cisco Unity Connection 10.x 29-2
Enabling Phone Access to the Broadcast Message Administrator in Cisco Unity Connection 10.x 29-2
Creating a Call Handler to Send Users to the Broadcast Message Administrator 29-3
Setting Up a One-Key Dialing Option to Send Users to the Broadcast Message Administrator 29-4
Setting Up a Special Phone Number and Routing Rule to Send Users to the Broadcast Message Administrator 29-5
Using the Broadcast Message Administrator in Cisco Unity Connection 10.x 29-6
Changing Broadcast Message Administrator Defaults in Cisco Unity Connection 10.x 29-7

CHAPTER 30 **Managing System Distribution Lists in Cisco Unity Connection 10.x** 30-1
Predefined System Distribution Lists in Cisco Unity Connection 10.x 30-1
Creating System Distribution Lists in Cisco Unity Connection 10.x 30-2
Modifying System Distribution Lists in Cisco Unity Connection 10.x 30-3

Managing System Distribution List Members in Cisco Unity Connection 10.x 30-4
Adding Alternate Names for a System Distribution List in Cisco Unity Connection 10.x 30-5
Using Advanced Settings to Enable System Distribution List Access Lists in Cisco Unity Connection 10.x 30-6

CHAPTER 31 **Managing Partitions and Search Spaces in Cisco Unity Connection 10.x 31-1**
Overview of Partitions in Cisco Unity Connection 10.x 31-1
Overview of Search Spaces in Cisco Unity Connection 10.x 31-2
Default Partition and Search Space in Cisco Unity Connection 10.x 31-3
Search Space Examples in Cisco Unity Connection 10.x 31-3
Single Site Automated Attendant Search Space Example 31-3
Multiple Site Search Space Example 31-4
How Search Spaces Work in Cisco Unity Connection 10.x 31-5
Search Spaces and Users 31-5
Search Spaces and Call Routing Rules 31-6
Search Spaces and System Distribution Lists 31-7
Search Spaces and System Call Handlers 31-7
Search Spaces and Directory Handlers 31-7
Search Spaces and Interview Handlers 31-7
Search Spaces and Networking in Cisco Unity Connection 10.x 31-8
Search Spaces and VPIM Locations 31-8
Search Spaces and Administrator-Defined Contacts 31-8
Managing Partitions in Cisco Unity Connection 10.x 31-9
Managing Search Spaces in Cisco Unity Connection 10.x 31-10
Changing the System Default Partition and Search Space in Cisco Unity Connection 10.x 31-11
Finding Objects that Belong to a Partition or Search Space in Cisco Unity Connection 10.x 31-11
Finding Objects Based on Partition in Cisco Unity Connection Administration 31-12
Finding Users Based on Partition in Cisco Unity Connection Serviceability 31-12

CHAPTER 32 **Managing the Phone System Integrations in Cisco Unity Connection 10.x 32-1**
Managing Phone Systems in Cisco Unity Connection 10.x 32-1
Adding a New Phone System Integration 32-2
Deleting a Phone System Integration 32-2
Changing Phone System Settings 32-3
Listing the Users Who Are Associated with the Phone System 32-3
Disabling the Use of the Same Port for Turning On and Off an MWI 32-4
Synchronizing MWIs for the Phone System 32-4
Configuring Phone View Settings (Cisco Unified Communications Manager Integrations Only) 32-4

Changing Call Loop Detection Settings 32-5
Managing AXL Servers 32-5
Managing Port Groups in Cisco Unity Connection 10.x 32-7
Adding a Port Group 32-8
Deleting a Port Group 32-8
Changing Port Group Settings 32-9
Changing the Audio Format That Cisco Unity Connection Uses for Calls 32-9
Changing the Video Format that Cisco Unity Connection 10.x Uses for Calls 32-10
Changing MWI Settings 32-11
Adding Secondary Cisco Unified Communications Manager Servers 32-11
Deleting Cisco Unified Communications Manager Servers 32-12
Changing Cisco Unified Communications Manager Server Settings 32-12
Adding a TFTP Server 32-13
Deleting a TFTP Server 32-13
Changing TFTP Server Settings 32-14
Adding a SIP Server 32-14
Deleting a SIP Server 32-15
Changing SIP Server Settings 32-15
Managing PIMG/TIMG Units 32-16
Changing Session Initiation Protocol (SIP) Settings 32-17
Changing Port Group Advanced Settings 32-17
Enabling or Disabling Normalization 32-17
Managing Ports in Cisco Unity Connection 10.x 32-18
Adding a Port 32-18
Deleting a Port 32-19
Changing Port Settings 32-19
Viewing the Port Certificate 32-21
Managing Speech Connect Port in Cisco Unity Connection 10.x 32-21
Configuring a Speech Connect Port 32-21
Managing Phone System Trunks in Cisco Unity Connection 10.x 32-22
Adding a Phone System Trunk 32-22
Deleting a Phone System Trunk 32-22
Changing Phone System Trunk Settings 32-23
Security in Cisco Unity Connection 10.x (Cisco Unified Communications Manager Integrations Only) 32-23
Viewing the Cisco Unity Connection Root Certificate 32-24
Saving the Cisco Unity Connection Root Certificate as a File 32-24
Adding a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-25

Deleting a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-25
Changing a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-26
Adding a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-26
Deleting a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-26
Changing a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only) 32-27
IPv6 in Cisco Unity Connection (Cisco Unified Communications Manager Integrations Only) 32-27

CHAPTER 33 **Creating a Cisco Unified Mobility Advantage Integration in Cisco Unity Connection 10.x** 33-1
About the Cisco Unified Mobility Advantage Integration in Cisco Unity Connection 10.x 33-1
Task List for Creating an Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage 33-1
Requirements 33-2
Configuring Cisco Unity Connection 10.x for a Cisco Unified Mobility Advantage Integration 33-2
Testing the Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage 33-3

CHAPTER 34 **Creating a Cisco Fax Server Integration in Cisco Unity Connection 10.x** 34-1
About the Cisco Fax Server Integration in Cisco Unity Connection 10.x 34-1
Task List for Creating a Cisco Fax Server Integration in Cisco Unity Connection 10.x 34-2
Requirements 34-2
Configuring the Cisco Fax Server in Cisco Unity Connection 10.x 34-3
Configuring Cisco Unity Connection 10.x for the Cisco Fax Server Integration 34-6
Configuring Cisco Unity Connection 10.x Users for the Cisco Fax Server Integration 34-7
Testing the Cisco Fax Server Integration in Cisco Unity Connection 10.x 34-7
Changing the Cisco Unity Connection 10.x Configuration for the Cisco Fax Server Integration 34-8
Changing the Cisco Unity Connection 10.x User Configuration for the Cisco Fax Server Integration 34-9
Configuring a Single Number to Receive Both Voice Calls and Faxes in Cisco Unity Connection 10.x 34-9
Task List 34-10
Requirements 34-10

CHAPTER 35 **Managing SpeechView Transcription Error Codes in Cisco Unity Connection** 35-1
Overview of SpeechView Transcription in Cisco Unity Connection 35-1
Default Transcription Error Codes in Cisco Unity Connection 35-2
Add New Transcription Error Code in Cisco Unity Connection 35-2

Modifying the Transcription Error Code in Cisco Unity Connection 35-3
Deleting the Transcription Error Code in Cisco Unity Connection 35-4
Search the Transcription Error Codes in Cisco Unity Connection 35-4

CHAPTER 36 **Creating Calendar and Contact Integrations in Cisco Unity Connection** 36-1
About Calendar Integrations in Cisco Unity Connection 36-1
About Contact Integrations in Cisco Unity Connection 36-2
Creating a Calendar and Contact Integration with Exchange 2007 in Cisco Unity Connection 36-2
Task List for Creating a Calendar and Contact Integration with Exchange 2007 in Cisco Unity Connection 36-2
Requirements for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection 36-3
Configuring Exchange 2007 for the Calendar and Contact Integration in Cisco Unity Connection 36-3
Configuring Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration 36-6
Configuring Users for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection 36-7
Testing the Exchange 2007 Calendar Integration in Cisco Unity Connection 36-8
Creating a Calendar and Contact Integration with Exchange 2003 in Cisco Unity Connection 36-9
Task List for Creating a Calendar and Contact Integration with Exchange 2003 in Cisco Unity Connection 36-9
Requirements for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection 36-10
Configuring Exchange 2003 for the Calendar and Contact Integration in Cisco Unity Connection 36-10
Configuring Cisco Unity Connection for the Exchange 2003 Calendar and Contact Integration 36-13
Configuring Users for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection 36-14
Testing the Exchange 2003 Calendar Integration in Cisco Unity Connection Do the following procedure. 36-15
Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace in Cisco Unity Connection 36-16
Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace in Cisco Unity Connection 36-16
Requirements for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection 36-16
Configuring Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection 36-17
Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration 36-18
Configuring Users for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection 36-19

Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection 36-20

Creating a Calendar Integration with Cisco Unified MeetingPlace Express in Cisco Unity Connection 36-21

Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace Express in Cisco Unity Connection 36-21

Requirements for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection 36-22

Configuring Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection 36-22

Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration 36-23

Configuring Users for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection 36-25

Testing the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection 36-26

CHAPTER 37 **Configuring Service Parameters in Cisco Unity Connection 10.x** 37-1

Configuring Service Parameters for a Cisco Unified Serviceability Service in Cisco Unity Connection 10.x 37-1

Description of Service Parameters in Cisco Unity Connection 10.x 37-2

CHAPTER 38 **Configuring Enterprise Parameters in Cisco Unity Connection 10.x** 38-1

Configuring Enterprise Parameters for Cisco Unified Serviceability Services in Cisco Unity Connection 10.x 38-1

Description of Enterprise Parameters in Cisco Unity Connection 10.x 38-2

CHAPTER 39 **Installing Plugins in Cisco Unity Connection 10.x** 39-1

CHAPTER 40 **Managing Descriptions of Message Attachments in Cisco Unity Connection 10.x** 40-1

Adding a Description of a Message Attachment in Cisco Unity Connection 10.x 40-1

Changing a Description of a Message Attachment in Cisco Unity Connection 10.x 40-2

Deleting a Description of a Message Attachment in Cisco Unity Connection 10.x 40-2

CHAPTER 41 **Setting Up Phone View in Cisco Unity Connection 10.x** 41-1

CHAPTER 42 **Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 10.x** 42-1

About Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 42-1

Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection 42-1

Task List for Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection 42-2
Enabling IMAP Access to Exchange in Cisco Unity Connection 42-2
Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only) 42-3
Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection 42-4
Configuring Users for the External Services in Cisco Unity Connection 42-5
Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection 42-6
Task List for Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection 42-7
Enabling IMAP Access to Exchange in Cisco Unity Connection 42-7
Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only) 42-8
Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only) 42-9
Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only) 42-14
Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only) 42-14
Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection 42-16
Configuring Users for the External Services in Cisco Unity Connection 42-17

CHAPTER 43 **Reports in Cisco Unity Connection 10.x** 43-1
Reports Overview in Cisco Unity Connection 10.x 43-1
Setting Report Configuration Parameters in Cisco Unity Connection 10.x 43-4
Archiving Report Data 43-5
Generating and Viewing Reports in Cisco Unity Connection 10.x 43-5

CHAPTER 44 **Integrating Cisco Unity Connection 10.x with an LDAP Directory** 44-1
Integrating Cisco Unified Communications Manager and Cisco Unity Connection 10.x with an LDAP Directory 44-2
Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 10.x Users with LDAP Users 44-2
Activating the Cisco DirSync Service in Cisco Unity Connection 10.x 44-4
Enabling LDAP Synchronization in Cisco Unity Connection 10.x 44-4
Disabling LDAP Synchronization in Cisco Unity Connection 10.x 44-5
Converting Phone Numbers into Extensions 44-5
Uploading SSL Certificates on the Cisco Unity Connection 10.x Server 44-7
Configuring LDAP Authentication in Cisco Unity Connection 10.x 44-8

Disabling LDAP Authentication 44-9
Selecting the LDAP Users to Import into Cisco Unity Connection 10.x 44-10
Directories Other than Active Directory 44-11
Active Directory 44-11
Cisco Unity Connection Intrasite and Intersite Networking 44-12
Filtering LDAP Users in Cisco Unity Connection 10.x 44-12
Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x 44-14
Changing LDAP Directory Configurations in Cisco Unity Connection 10.x 44-15
Deleting LDAP Directory Configurations in Cisco Unity Connection 10.x 44-16
Changing Which LDAP Field Is Mapped to the Alias Field in Unity Connection 44-16

CHAPTER 45 **Setting up Tenant Partitioning in Cisco Unity Connection 10.x 45-1**
Introduction to Tenant Partitioning 45-1
Tenant Provisioning using APIs 45-1
Working with Tenant Partitioning 45-2
Phone System Integration 45-3
Modifying the Objects after Tenant Creation 45-3

CHAPTER 46 **Managing Licenses in Cisco Unity Connection 10.x 46-1**
About Licenses in Cisco Unity Connection 10.x 46-1
License Management and Enterprise License Manager (ELM) in Cisco Unity Connection 10.x 46-1
Licenses and Cisco Unity Connection Clusters 46-3
Licenses and Migrations from Cisco Unity 46-3
Viewing Reports for Licenses in Cisco Unity Connection 10.x 46-3
Viewing the License Status for Cisco Unity Connection 46-3
Viewing the Last Connectivity Time with the ELM Server 46-4
Viewing the Host Name/ IP Address of the Connected ELM Server 46-4
Viewing the Last Compliance Time 46-5
Viewing the License Usage 46-5
License Parameters for Cisco Unity Connection 10.x Features 46-5

CHAPTER 47 **Managing Cisco Unity Connection Survivable Remote Site Voicemail in Cisco Unity Connection 10.x 47-1**
Overview of Cisco Unity Connection SRSV in Unity Connection 10.x 47-1
Working with Unity Connection SRSV 47-2
Supported SRSV Topologies 47-2
Methods of Provisioning and Voicemail Upload 47-5
Configuring an SRSV User 47-6

Managing Branches in Cisco Unity Connection 10.x 47-6

CHAPTER 48 **Shortcut Keys for Cisco Unity Connection Administration 48-1**

Other Unity Connection Features 48-3

Speech Connect for Cisco Unity Connection 48-4

Cisco SpeechView 48-4

TTY Overview 48-4

48-5

INDEX

# Preface

## Audience and Use

The *System Administration Guide for Cisco Unity Connection* contains information and instructions for creating a call management plan by using call routing, restriction tables, and call handlers; for customizing the Cisco Unity Connection conversation; for handling messages and distribution lists; for managing audio formats; for managing user passwords and PINs; for managing the phone system integration; for setting up system transfers; for configuring IMAP settings; for managing partitions and search spaces; and for creating a Cisco Fax Server integration.

For a detailed listing of all settings in Cisco Unity Connection Administration, see the *Interface Reference Guide for Cisco Unity Connection Administration*.

For information and instructions for creating, modifying, and deleting user accounts and templates, see the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For information and instructions for setting up user workstations, see the *User Workstation Setup Guide for Cisco Unity Connection*.

For information and instructions for setting up networking, including VPIM networking, see the *Networking Guide for Cisco Unity Connection*.

These guides are all available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

## Documentation Conventions

*Table 1 Conventions in the System Administration Guide for Cisco Unity Connection*

| Convention | Description |
|---|---|
| boldfaced text | Boldfaced text is used for:<br>• Key and button names. (Example: Select **OK**.)<br>• Information that you enter. (Example: Enter **Administrator** in the Username box.) |
| < ><br>(angle brackets) | Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to **https://<Cisco Unity Connection server IP address>/cuadmin**.) |

*Table 1 Conventions in the System Administration Guide for Cisco Unity Connection*

| Convention | Description |
|---|---|
| - (hyphen) | Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.) |
| > (right angle bracket) | A right angle bracket is used to separate selections that you make in the navigation bar of Cisco Unity Connection Administration. (Example: In Cisco Unity Connection Administration, expand **Contacts > System Contacts**.) |

The *System Administration Guide for Cisco Unity Connection* also uses the following conventions:

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

**Tip** Means the following information may help you solve a problem.

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

# Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Unity Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/roadmap/10xcucdg.html.

# Documentation References to Cisco Unified Communications Manager Business Edition (CMBE)

The name of the product known as Cisco Unified Communications Manager Business Edition in versions 8.0 and earlier has been changed to Cisco Unified Communications Manager Business Edition 5000 in versions 8.5 and later.

In Cisco Unity Connection 10.x documentation set, references to “Cisco Unified Communications Manager Business Edition (CMBE)” and “Cisco Unified CMBE” apply on Business Edition 6000. The references do not apply on any other Business Editions.

# Obtaining Documentation and Submitting a Service Request

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

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

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

# Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

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

# Configuring the Browser on a Cisco Unity Connection 10.x Administrator Workstation

To access Cisco Unity Connection Administration, Cisco Unified Serviceability, Cisco Unity Connection Serviceability, Disaster Recovery System, and other web applications on the Unity Connection server, the web browsers must be set up correctly on an administrator workstation.

See the applicable section, depending on the web browsers installed on the computer:

- Configuring Firefox on a Cisco Unity Connection 10.x Administrator Workstation, page 1-1
- Configuring Microsoft Internet Explorer on a Cisco Unity Connection 10.x Administrator Workstation, page 1-2

**Note**

- Make sure to run trusted sites while opening Cisco Unity Connection Administration, Cisco Personal Communications Assistant, and Web Inbox.
- We recommend that you use the hostname for accessing Cisco Unity Connection.

## Configuring Firefox on a Cisco Unity Connection 10.x Administrator Workstation

Do the following tasks to set up Firefox for accessing the Cisco Unity Connection web applications.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements—Administrator Workstations" section of *System Requirements for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
2. Configure Firefox:
   a. Enable **Java**.
   b. Enable **Java Script** > Enable **Change Images in Java Script Advanced**.
   c. Allow sites to set cookies. (For security purposes, we recommend that you set this to **Allow Sites to Set Cookies for the Originating Web Site Only**.)

# Configuring Microsoft Internet Explorer on a Cisco Unity Connection 10.x Administrator Workstation

Do the following tasks to set up Internet Explorer for accessing the Cisco Unity Connection web applications.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements—Administrator Workstations" section *System Requirements for Cisco Unity Connection Release 10.x*, available at: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html
   - Configure Internet Explorer:
   a. Enable **Active scripting**.
   b. Download and run **ActiveX controls**.
   c. Enable **Java scripting.**
   d. Accept all cookies.
   e. Automatically check for newer versions of temporary Internet files.
   f. Enable Medium-High privacy.
   g. If you are running Microsoft Windows Server 2003 and using Internet Explorer version 6.0 to access the Cisco PCA, add the Unity Connection server to the Trusted Sites list by doing the steps mentioned in next section.

**Note** Microsoft Internet Explorer 7.0, 8.0, and 9.0 versions support both the IPv4 and IPv6 addresses on Windows XP, Windows Vista, and Windows 7 operating systems. However, the IPv6 address works only when Unity Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrug051.html.

### To Add the Cisco Unity Connection Server to the List of Trusted Sites (Windows Server 2003 with Internet Explorer 6.0 Only)

**Step 1** Open the Cisco Personal Communications Assistant Sign-in page. It is not necessary to sign in to the Cisco PCA.

**Step 2** On the **Internet Explorer File** menu, select **Add This Site To > Trusted Sites Zone**.

**Step 3** In the **Trusted Sites** dialog box, select **Add**.

**Step 4** Select **Close** to close the **Trusted Sites** dialog box.

**Step 5** Restart **Internet Explorer**.

# Accessing and Using Cisco Unity Connection Administration 10.x

Cisco Unity Connection Administration is a web application that you use to do most administrative tasks, including specifying settings for users, and implementing a call management plan.

See the following sections:


- Accessing and Exiting Cisco Unity Connection Administration 10.x, page 2-1
- Cisco Unity Connection Administration 10.x User Interface, page 2-2
- Using Cisco Unity Connection Administration 10.x Help, page 2-3
- Finding Records in Cisco Unity Connection Administration 10.x, page 2-3
- Accessing Other Cisco Unity Connection Administration 10.x Locations in the Network, page 2-4


For information on configuring the browser on the administrator workstation, see the "Configuring the Browser on a Cisco Unity Connection 10.x Administrator Workstation" chapter.

**Note** Cisco Unity Connection Administration supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Unity Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrug051.html.

# Accessing and Exiting Cisco Unity Connection Administration 10.x

The first time that you sign in to Cisco Unity Connection Administration, you use the username and password for the default administrator account that the installer specified for the account during installation. Later, you can use the username and password for any additional administrator accounts that you create.

By default, a Unity Connection Administration session is set to time out after twenty minutes. You can change the Administration Session Timeout setting on the **System Settings > Advanced > Unity Connection Administration** page.

**Note** You can also administer accounts on other Unity Connection servers in the network. See the "Accessing Other Cisco Unity Connection Administration 10.x Locations in the Network" section on page 2-4.

### To Sign In to Cisco Unity Connection Administration

**Step 1** On an administrator workstation, open a browser session.

**Step 2** Go to **https://<Cisco Unity Connection server IP address>/cuadmin**.

**Note** We recommend that you bookmark Unity Connection Administration. If a Unity Connection cluster is configured, we recommend that you bookmark this page for both Unity Connection servers so that you can sign in to Unity Connection Administration on the functional server when the other Unity Connection server is not functioning.

**Step 3** Enter an applicable username and password, and select **Sign-In**.

### To Exit Cisco Unity Connection Administration

**Step 1** In the Cisco Unity Connection Administration title pane, select **Sign Out**.

**Step 2** Exit the web browser.

# Cisco Unity Connection Administration 10.x User Interface

The Cisco Unity Connection Administration interface is divided into four areas.

| | |
|---|---|
| **Navigation pane** | Located along the left side of the interface; contains links to the Unity Connection Administration pages. Select the name of the page to display it. |
| **Title pane** | Located across top of the interface; contains an About link and the Sign Out link.<br>The title pane also offers a Navigation menu that you can use to browse to other Cisco applications. Select the name of the application from the Navigation list, and then select Go. Depending on the application, you may be required to sign in. |
| **Title bar** | Displays the name of the page and, if applicable, the name of the record displayed on the page. For example, on the Edit User Basics page for a user with the alias GreetingsAdmin, the title bar reads "Edit User Basics (GreetingsAdmin)." The right side of the title bar also shows the navigation path of the page, as it relates to other pages in the category. You can select a page in the navigation path to go that page. |
| **Page** | Where Unity Connection data is entered and displayed. The page name appears in the title bar at the top of the page. |

# Using Cisco Unity Connection Administration 10.x Help

To access **Help**, select the **Help** menu at the top of a page in Cisco Unity Connection Administration, and select one of the following:

| | |
|---|---|
| **Contents** | Opens a new browser window, and displays the home page for the Cisco Unity Connection Administration Help system. The links in the left pane of the Help window allow you to access all topics in the Help system. |
| **This Page** | Opens a new browser window for the Cisco Unity Connection Administration Help system. The right pane of the window contains definitions for each field on the current page in Unity Connection Administration. In most cases there are cross-references to additional topics related to the current page.<br><br>The left pane of the Help system provides a table of contents for all of the product guides included in Help. The table of contents expands to show the location within the hierarchy of the Help topic that is displayed on the right. |

To learn more about the Unity Connection Help system—including instructions on how to search Help, select the Using **Help** link at the top of any **Help** page.

# Finding Records in Cisco Unity Connection Administration 10.x

A record is the group of settings or collection of data for an individual user, class of service, call handler, or other Cisco Unity Connection entity. For example, a user record contains the user account data.

Cisco Unity Connection Administration lets you find records based on search criteria that you enter. As a best practice, do not use wildcards such as * in search strings. When you want to find a user or contact, use Begins With, Contains, or Ends With to match part of a string, or leave the search string blank to return all results. Unity Connection attempts to match wildcard characters within the field you are searching; if no objects contain such characters in that field, no results are returned.

You can use the navigation buttons at the bottom of the search results table to move between pages, and the Rows Per Page setting to display 25, 50, 100, 150, 200, or 250 rows per page. Unity Connection saves your Rows Per Page setting, so that on subsequent sign-ins you receive the same number of results per page for this search page.

### To Find a User Account

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, in the **Search Results** table, select the user alias to display the user account.

If you do not see the user alias listed in the **Search Results** table, continue with Step 3.

**Step 3** In the **Find Users** where search fields, indicate whether to search by Alias, DTMF Access ID, First Name, Last Name, or Display Name. You can further refine your search by setting additional parameters such as Begins With or Ends With. Enter the applicable characters to search for, and select **Find**.

**Step 4** In the **Search Results** table, select the user alias to display the user account.

### To Find Other Types of Cisco Unity Connection Data

**Step 1** In Cisco Unity Connection Administration, go to the applicable **Search** page.

**Step 2** If the applicable record is listed in the **Search Results** table, select the record name to display the record.

If you do not see the record listed in the **Search Results** table, continue with Step 3.

**Step 3** In the search fields, indicate the search parameters, and enter the applicable characters to search for. Select **Find**.

**Step 4** In the **Search Results** table, select the record name to display the record.

# Accessing Other Cisco Unity Connection Administration 10.x Locations in the Network

From the local server in your network, you can access other networked servers, and can edit the following types of information on the remote servers:

- User Accounts
- Contacts
- Distribution lists
- Locations
- Partitions
- Search spaces

On your local server, any remote objects in the network are identified on the page by the color of the icon next to the object name. When you select a remote object, the Status message at the top of the page tells you that the object is homed on a remote server, and includes a link to the remote server. Select the link, and sign in with the applicable administrative credentials. When you have signed in, the object that you selected opens in a separate browser window and you can edit the object as usual.

When you edit objects on remote servers, the updates replicate to other servers in the network, depending on the synchronization settings for your network; updates may not occur until the next scheduled task run. If you want to immediately synchronize the data, do any one of the following procedures depending upon the type of the network (Legacy or HTTPS network).

### To Immediately Begin Directory Synchronization in Legacy Network

Legacy networking further includes Intrasite networking and Intersite networking.

Do the following steps to begin synchronization in an Intrasite network.

**Step 1** In Cisco Unity Connection Administration, expand **Networking** > **Legacy Links**, and select **Intrasite Links**.

**Step 2** On the **Search Intrasite Links** page, locate the applicable server in the network.

**Step 3** Select **Push Directory To** or **Pull Directory From** to immediately push or pull the directory information.

Do the following steps to begin synchronization in an Intersite network.

**Step 1** In Cisco Unity Connection Administration, expand **Networking** > **Legacy Links**, and select **Intersite Links**.

**Step 2** On the **Search Intersite Links** page, locate the applicable server in the network.

**Step 3** Under **Synchronization**, select **Sync**.

#### To Immediately Begin Directory Synchronization in an HTTPS Network

**Step 1** In Cisco Unity Connection Administration, expand **Networking** and select **HTTPS Links**.

**Step 2** On the **Search HTTPS Links** page, locate the applicable server in the network.

**Step 3** Under **Synchronization**, select **Sync**.

# Administrative Tools in Cisco Unity Connection 10.x

This chapter provides brief descriptions of and procedures for accessing a selection of tools and utilities for administering Cisco Unity Connection. (To configure a browser to access Unity Connection web applications, see the "Configuring the Browser on a Cisco Unity Connection 10.x Administrator Workstation" chapter.)

See the following sections:


- Application Plug-ins in Cisco Unity Connection 10.x, page 3-2
- Cisco Unified Backup and Restore Application Suite (COBRAS) in Cisco Unity Connection 10.x, page 3-2
- Cisco Unity Connection Administration 10.x, page 3-2
- Cisco Unity Connection 10.x Bulk Administration Tool, page 3-3
- Cisco Unity Connection 10.x Custom Keypad Mapping Tool, page 3-3
- Cisco Unity Connection 10.x Grammar Statistics Tool, page 3-4
- Cisco Unity Connection 10.x Import and Synch Users Tools, page 3-4
- Cisco Unity Connection 10.x Migrate Messages Utility, page 3-5
- Cisco Unity Connection 10.x Migrate Users Utility, page 3-5
- Cisco Unity Connection Serviceability 10.x, page 3-6
- Cisco Unity Connection 10.x Show Dependency Results, page 3-6
- Cisco Unity Connection 10.x Task Management Tool, page 3-6
- Disaster Recovery System in Cisco Unity Connection 10.x, page 3-7
- Cisco Voice Technology Group Subscription Tool in Cisco Unity Connection 10.x, page 3-7
- Real-Time Monitoring Tool in Cisco Unity Connection 10.x, page 3-7
- Cisco Unified Serviceability in Cisco Unity Connection 10.x, page 3-8
- Remote Database Administration Tools in Cisco Unity Connection 10.x, page 3-8
- Cisco Utilities Database Link for Informix (CUDLI) in Cisco Unity Connection 10.x, page 3-9
- Unity Connection User Data Dump (CUDD) in Cisco Unity Connection 10.x, page 3-10
- Wallet Card Wizard in Cisco Unity Connection 10.x, page 3-10

# Application Plug-ins in Cisco Unity Connection 10.x

Application plug-ins extend the functionality of Cisco Unity Connection. For example, the Real-Time Monitoring Tool (RTMT) plug-in allows an administrator to monitor system performance.

For Cisco Unity Connection configurations, see the "Installing Plugins in Cisco Unity Connection 10.x" chapter for detailed information.

# Cisco Unified Backup and Restore Application Suite (COBRAS) in Cisco Unity Connection 10.x

Cisco Unified Backup and Restore Application Suite (COBRAS) is the application you use to migrate data and messages from Cisco Unity 4.0(5) or later or from Cisco Unity Connection 1.2 to Unity Connection 10.x. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

Alternatively, you can use the Cisco Unity Connection Migrate Messages and Migrate Users utilities to migrate messages and user data when you are migrating from Cisco Unity 4.0(4) and earlier and you cannot upgrade to Cisco Unity 4.0(5) or later for some reason. COBRAS migrates significantly more data than the Migrate Users utility, and it does not require that you configure a secure shell (SSH) server application. For more information, see the "Cisco Unity Connection 10.x Migrate Messages Utility" section on page 3-5 and the "Cisco Unity Connection 10.x Migrate Users Utility" section on page 3-5.

**Note** Migration in a Tenant Partitioned environment using COBRAS tool allows the administrator to export the data from a non-partitioned Unity Connection system or a Tenant-Partitioned Unity Connection system. For more information on each scenario and on migration process using COBRAS tools, refer to http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html link.

For a task list that enumerates the steps for migrating from Cisco Unity or from Unity Connection 1.x to Unity Connection 10.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the applicable chapter of the *Upgrade Guide for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html.

# Cisco Unity Connection Administration 10.x

Cisco Unity Connection Administration is a web application that you use to do most administrative tasks, including specifying settings for users and implementing a call management plan. Many of the tools listed in this section are available from Connection Administration.

For information on accessing and using Cisco Unity Connection Administration, see the "Accessing and Using Cisco Unity Connection Administration 10.x" chapter.

# Cisco Unity Connection 10.x Bulk Administration Tool

The Cisco Unity Connection Bulk Administration Tool (BAT) allows you to create, update, and delete multiple user accounts, administrator-defined contacts, system distribution lists, or system distribution list members at the same time by importing information contained in a comma separated value (CSV) file. In addition, it allows you to export information about users, administrator-defined contacts, system distribution lists, system distribution list members, or LDAP users from Cisco Unity Connection to a CSV file.

> For small numbers of users—up to a few hundred—it may be faster and easier to use the Import Users tool to create Unity Connection users from users in an LDAP directory. See the "Cisco Unity Connection 10.x Import and Synch Users Tools" section on page 3-4.

### To Access the Cisco Unity Connection Bulk Administration Tool

**Step 1** In Cisco Unity Connection Administration, expand **Tools**.

**Step 2** Select **Bulk Administration Tool**.

For information on using the BAT tool on Unity Connection or Cisco Unified CMBE, see the "Using the Cisco Unity Connection 10.x Bulk Administration Tool" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Cisco Unity Connection 10.x Custom Keypad Mapping Tool

The Custom Keypad Mapping tool allows you to edit the key mappings that are associated with the Custom Keypad Mapping conversation, which can be assigned to users or user templates on the Phone Menu page in Cisco Unity Connection Administration. You are allowed to assign any one-, two-, or three-key sequence to any defined option for the main menu, the message playback menu (the message header, body, and footer can be mapped separately), the after message menu, and the settings menu. You can customize which options are voiced in each menu and the order in which they are offered. The Custom Keypad Mapping tool is accessed in the Tools section of Connection Administration.

### To Access the Custom Keypad Mapping Tool

**Step 1** In Cisco Unity Connection Administration, expand **Tools**.

**Step 2** Select **Custom Keypad Mapping**.

For information on using the tool, see the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter.

# Cisco Unity Connection 10.x Grammar Statistics Tool

The Grammar Statistics tool shows information about all of the dynamic name grammars that are used by the Cisco Unity Connection voice-recognition conversation to match caller utterances to the names of objects on the system (for example, usernames and alternate names, distribution list names, and so on). When administrators add or change names on the Unity Connection system, the names are not recognized by the voice-recognition conversation until they are compiled in the grammars.

For each name grammar, the tool displays information such as the finish time of the last grammar recompilation, the total number of unique items in the grammar, whether there are updates pending to the grammar, and whether the grammar is currently in the process of being recompiled.

By default, Unity Connection recompiles grammars when administrators add named objects or change object names on the system (unless a bulk operation is in progress, in which case Unity Connection waits ten minutes for the operation to complete before recompiling the grammars), or when there are more than five changes requested in the space of a minute. If the grammars have grown to the point where the name grammar recompilation process is affecting the performance of your Unity Connection server during busy periods, you can modify the default Voice Recognition Update Schedule (under **System Settings > Schedules** in Cisco Unity Connection Administration) to limit the times and days when the Unity Connection voice-recognition transport utility can automatically rebuild the voice-recognition name grammars. By default, all days and times are active for this schedule; if you modify the schedule but want to override the schedule while it is inactive and force an immediate recompilation of all grammars, or if you want to force recompilation during the ten minute wait period after a bulk operation has been initiated, you can select the Rebuild Grammars button on the Grammar Statistics tool.

# Cisco Unity Connection 10.x Import and Synch Users Tools

When the Cisco Unity Connection server is integrated with a Cisco Unified Communications Manager phone system, you can use the Import Users tool to automatically create multiple users with voicemail accounts from existing Cisco Unified Communications Manager users.

You can also use the Import Users tool to create small numbers of users—up to a few hundred—from users in an LDAP directory. (This is not a question of technical limitations; you can create many thousands of users by using the Import Users tool, but the process is less efficient than other methods.)

In Cisco Unity Connection configurations, the Synchronize Users tool allows you to manually refresh the information you imported from Cisco Unified Communications Manager when you created voicemail users.

In Cisco Unified Communications Manager Business Edition (CMBE) configurations, synchronization happens automatically. There should be no need to manually synchronize users.

### To Access the Import and Synch Users Tools

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

**Step 2** Select **Import Users** or **Synch Users**, as applicable.

For information on using both tools, see the "Creating Multiple Cisco Unity Connection 10.x User Accounts from Cisco Unified Communications Manager Users" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Cisco Unity Connection 10.x Migrate Messages Utility

To migrate messages and data from Cisco Unity 4.0(5) or later to Unity Connection 10.x, we recommend that you use the Cisco Unified Backup and Restore Application Suite (COBRAS) tool instead of the Migrate Messages and Migrate Users utilities. COBRAS migrates significantly more data than the Migrate Users utility, and it does not require that you configure a secure shell (SSH) server application. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

For a task list that enumerates the steps for migrating from Cisco Unity to Unity Connection 10.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the "Migrating from Cisco Unity 4.x or Later to Cisco Unity Connection 10.x" chapter of the *Upgrade Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html.

The Cisco Unity Connection Migrate Messages utility allows you to migrate messages from Cisco Unity to Cisco Unity Connection 10.x. You can only migrate messages if you have first migrated user data by using the Migrate Users utility.

### To Access the Migrate Messages Utility (Cisco Unity Connection Configurations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Tools**.

**Step 2** Expand **Migration Utilities**, then select **Migrate Users**.

# Cisco Unity Connection 10.x Migrate Users Utility

To migrate messages and data from Cisco Unity 4.0(5) or later to Unity Connection 10.x, we recommend that you use the Cisco Unified Backup and Restore Application Suite (COBRAS) instead of the Migrate Messages and Migrate Users utilities. COBRAS migrates significantly more data than the Migrate Users utility, and it does not require that you configure a secure shell (SSH) server application. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

For a task list that enumerates the steps for migrating from Cisco Unity to Unity Connection 10.x either by using COBRAS or by using the Migrate Messages and Migrate Users utilities, see the "Migrating from Cisco Unity 4.x or Later to Cisco Unity Connection 10.x" chapter of the *Upgrade Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html.

### To Access the Migrate Users Utility (Cisco Unity Connection Configurations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Tools**.

**Step 2** Expand **Migration Utilities**, then select **Migrate Users**.

# Cisco Unity Connection Serviceability 10.x

Cisco Unity Connection Serviceability, a web-based troubleshooting tool for Cisco Unity Connection, provides the following functionality:

- Displaying Unity Connection alarm definitions, which you can use for troubleshooting.
- Enabling Unity Connection traces. You can collect and view trace information in the Real-Time Monitoring Tool (RTMT) or in the command line interface (CLI).
- Configuring the logs to which Unity Connection trace information is saved.
- Viewing and changing the server status of the Unity Connection servers when a Unity Connection cluster is configured.
- Viewing the status of the Unity Connection feature services.
- Activating, deactivating, starting, and stopping the Unity Connection services.
- Generating reports that can be viewed in different file formats.

Depending on the service and component involved, you may perform serviceability-related tasks in both Cisco Unity Connection Serviceability and Cisco Unified Serviceability. For example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

For more information, see the *Administration Guide for Cisco Unity Connection Serviceability Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/serv_administration/guide/10xcucservagx.html.

# Cisco Unity Connection 10.x Show Dependency Results

The Show Dependency Results page provides a way to view the results of the most recent dependency search.

When database objects such as user accounts are referenced by other objects in Cisco Unity Connection (for example, if a user is set to be a recipient of messages left in an interview handler, or if a call handler is set to transfer incoming calls to a user phone), you cannot delete the referenced objects until you have changed settings on the dependent objects.

To determine the dependencies of an object that you want to delete, select the Show Dependencies option on the search page for the object type. The option initiates a search for database objects that are dependent on the object you want to delete. From the dependency search results, follow links to the dependent objects and reassign the dependencies. When all dependencies have been reassigned, you can delete the object.

Some dependency searches can take several minutes, depending on the object being searched. While a search is in progress, if you browse to another page, or your browser session times out, navigate to **Tools > Show Dependency Results** to view the dependency search results.

# Cisco Unity Connection 10.x Task Management Tool

The Task Management pages list a variety of system maintenance and troubleshooting tasks that Cisco Unity Connection automatically runs on a regular schedule. Tasks can be run at the same time as backups and anti-virus scans.

The default settings and schedules for each task are optimized for functionality and performance. We recommend that you not change the default settings and schedules.

**Caution** Some tasks are critical to Unity Connection functionality. Disabling or changing the frequency of critical tasks may adversely affect performance or cause Unity Connection to stop functioning.

**To Access the Task Management Tool**

**Step 1** In Cisco Unity Connection Administration, expand **Tools**.

**Step 2** Select **Task Management**.

# Disaster Recovery System in Cisco Unity Connection 10.x

Disaster Recovery System lets you back up and, if necessary, restore data and voice messages on a Cisco Unity Connection or Cisco Unified Communications Manager Business Edition system. For more information, see the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/drs_administration/guide/10xcucdrsag.html.

# Cisco Voice Technology Group Subscription Tool in Cisco Unity Connection 10.x

You can use the Cisco Voice Technology Group Subscription tool to be notified by email of any Cisco Unity Connection software updates. To subscribe, go to the Cisco Voice Technology Group Subscription Tool page at http://www.cisco.com/cgi-bin/Software/Newsbuilder/Builder/VOICE.cgi.

# Real-Time Monitoring Tool in Cisco Unity Connection 10.x

The Real-Time Monitoring Tool (RTMT), which runs as a client-side application, uses HTTPS and TCP to monitor system performance, device status, device discovery, and CTI applications for Cisco Unity Connection. RTMT can connect directly to devices via HTTPS to troubleshoot system problems. RTMT can also monitor the voice messaging ports on Unity Connection.

RTMT allows you to do the following tasks:

- Monitor a set of predefined management objects that focus on the health of the system.
- Generate various alerts, in the form of emails, for objects when values go over or below user-configured thresholds.
- Collect and view traces in various default viewers that exist in RTMT.
- View syslog messages and alarm definitions in SysLog Viewer.
- Work with performance-monitoring counters.

- Monitor the voice messaging ports on Unity Connection. When a Unity Connection cluster is configured, you can open multiple instances of RTMT to monitor voice messaging ports on each server in the Unity Connection cluster.

For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

# Cisco Unified Serviceability in Cisco Unity Connection 10.x

Cisco Unified Serviceability, a web-based troubleshooting tool for Cisco Unity Connection, provides the following functionality:

- Saving alarms and events for troubleshooting and providing alarm message definitions.
- Saving trace information to various log files for troubleshooting.
- Providing feature services that you can turn on, turn off, and view through the Service Activation window.
- Providing an interface for starting and stopping feature and network services.
- Generating and archiving daily reports; for example, alert summary or server statistic reports.
- Monitoring the number of threads and processes in the system; uses cache to enhance the performance.

Depending on the service and component involved, you may perform serviceability-related tasks in both Cisco Unified Serviceability and Cisco Unity Connection Serviceability. For example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

For more information, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

# Remote Database Administration Tools in Cisco Unity Connection 10.x

A database proxy can be enabled to allow the use of some Windows-based remote database administration tools that are available on the Cisco Unity Tools website (http://ciscounitytools.com), where updates to utilities are frequently posted between Cisco Unity Connection releases.

See the following sections for detailed information:

- Enabling Database Access for Remote Administration Tools, page 3-9
- Cisco Utilities Database Link for Informix (CUDLI) in Cisco Unity Connection 10.x, page 3-9
- Unity Connection User Data Dump (CUDD) in Cisco Unity Connection 10.x, page 3-10
- Wallet Card Wizard in Cisco Unity Connection 10.x, page 3-10

**Note** You can sign up to be notified when the utilities posted on the Cisco Unity Tools website are updated. Go to http://ciscounitytools.com and select **Sign Up Here**.

# Enabling Database Access for Remote Administration Tools

In order to use the remote tools, you must first enable remote database access. Because opening up database access for remote administration tools can introduce a security risk to your system, several layers of security are involved with enabling access:

- The username and password of a user with the Remote Administrator role is required to run remote tools.
- The Unity Connection Database Proxy service is disabled by default.

To enable remote database access, do the following three procedures in the order presented:

- To Assign the Remote Administrator Role to One or More Users, page 3-9
- To Start the Database Proxy Service, page 3-9

### To Assign the Remote Administrator Role to One or More Users

**Step 1** In Cisco Unity Connection Administration, select **Users**.

**Step 2** On the **Search Users** page, find the applicable user account.

**Note** As a best practice, do not use the default system administrator user account for remote access. Instead, use a different administrative user account to avoid having the default system administrator account become locked due to too many failed authentication attempts.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **Roles**.

**Step 4** On the **Edit Roles** page, in the **Available Roles** field, select **Remote Administrator**, then select the Up arrow to move it into the **Assigned Roles** field.

**Step 5** Select **Save**.

**Step 6** Repeat Step 2 through Step 5 for each user who needs access to remote administration tools.

### To Start the Database Proxy Service

**Step 1** In Cisco Unity Connection Serviceability, select **Tools > Service Management**.

**Step 2** In the **Optional Services** section, find the **Unity Connection Database Proxy** row and select **Activate**.

# Cisco Utilities Database Link for Informix (CUDLI) in Cisco Unity Connection 10.x

The Cisco Utilities Database Link for Informix (CUDLI) tool allows you to navigate the Cisco Unity Connection database, learn about the purpose of data in a particular table or column, and jump between referenced objects in the database. It also shows stored procedures and includes a custom query builder.

Download the tool and view training videos and Help at http://www.ciscounitytools.com/Applications/CxN/CUDLI/CUDLI.html.

# Unity Connection User Data Dump (CUDD) in Cisco Unity Connection 10.x

The Unity Connection User Data Dump (CUDD) allows you to export specific information about users to a file that can then be viewed or imported into another application such as a database utility or Excel. When the data is exported, the tool automatically creates a header row that lists the data type found in each column of the output, for ease of import into other programs.

Download the tool and view training videos and Help at http://www.ciscounitytools.com/Applications/CxN/UserDataDump/UserDataDump.html.

# Wallet Card Wizard in Cisco Unity Connection 10.x

The Wallet Card wizard is available for producing a PDF file of a wallet card based on any of the Unity Connection conversations, including custom keypad mappings. The templates in the wizard list frequently used menu options and shortcuts for managing Unity Connection messages and user preferences by phone; the wizard fills in the applicable keys based on the conversation that you specify. The resulting PDF is formatted as a wallet card that can be printed, then cut out and folded by users.

The wizard also allows you to customize technical support information and instructions for signing in to Unity Connection. The Wallet Card wizard is a Windows-based remote database administration tool. Download the tool and view Help at http://www.ciscounitytools.com/Applications/CxN/WalletCardWizard/WalletCardWizard.html.

# Call Management Overview in Cisco Unity Connection 10.x

Cisco Unity Connection provides a number of different call management elements that you can combine to customize how your system handles calls and collects input from callers.

See the following sections:


- Overview of Call Management Concepts in Cisco Unity Connection 10.x, page 4-1
- Call Handlers in Cisco Unity Connection 10.x, page 4-2
- Directory Handlers in Cisco Unity Connection 10.x, page 4-3
- Interview Handlers in Cisco Unity Connection 10.x, page 4-3
- Call Routing Tables in Cisco Unity Connection 10.x, page 4-4
- Restriction Tables in Cisco Unity Connection 10.x, page 4-6
- Schedules and Holidays in Cisco Unity Connection 10.x, page 4-8
- Default Cisco Unity Connection 10.x Automated Attendant Behavior, page 4-9


After reading about call management concepts, see the "Creating a Call Management Plan in Cisco Unity Connection 10.x" chapter for instructions on developing a plan.

## Overview of Call Management Concepts in Cisco Unity Connection 10.x

Cisco Unity Connection provides the following elements for managing incoming and outgoing calls:

| | |
|---|---|
| **Call Handlers** | Answer calls and can take messages; provide menus of options (for example, "For customer service press 1, for sales press 2..."); route calls to users and to other call handlers; and play audiotext (prerecorded information). |
| **Directory Handlers** | Provide access to a corporate directory by playing an audio list that users and outside callers use to reach users and to leave messages. |
| **Interview Handlers** | Collect information from callers by playing a series of questions and then recording the answers. |

| | |
|---|---|
| **Call Routing Tables** | Allow you to define how calls are initially routed, based on criteria such as the phone number of the caller and the schedule. When you have set up call handlers, interview handlers, and directory handlers, as well as extensions for users, you can route calls to the applicable person or handler by modifying the call routing tables. |
| **Restriction Tables** | Control outgoing calls by allowing you to specify the numbers that Unity Connection can dial for transferring calls, for notifying users of messages, and for delivering faxes. |
| **Schedules and Holidays** | Define business/nonbusiness and holiday hours for the organization, for the purpose of controlling which set of call routing rules, greetings, or transfer options is currently active. |

All of these elements can be used as building blocks; you can use or customize the default objects in Unity Connection, or add new objects and combine them to create the caller experience.

# Call Handlers in Cisco Unity Connection 10.x

Call handlers answer calls, greet callers with recorded prompts, provide callers with information and options, route calls, and take messages. They are a basic component of Cisco Unity Connection. Your plan for call handlers can be simple, using only the predefined call handlers, or you can create up to 40,000 new call handlers. You may want to use call handlers in the following ways:

- **As an automated attendant**—A call handler can be used in place of a human operator to answer and direct calls by playing greetings and responding to key presses. The automated attendant can provide a menu of options (for example, “For Sales, press 1; for Service, press 2; for our business hours, press 3.”).
- **To offer prerecorded audiotext**—A call handler can be used to provide information that customers request frequently (for example, “Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.”), or to play a prerecorded message that all callers hear before they can interact with the system.
- **As a message recipient—**A call handler can be used to take messages for the organization (for example, “All of our customer service representatives are busy. Please state your name, phone number, and account number, and we will return your call as soon as possible.”).
- **To transfer calls**—A call handler can be used to route callers to a user (for example, after hours, you could transfer calls that come to a technical support call handler directly to the mobile phone of the person who is on call), or to another call handler.

**Note** Cisco Unity Connection supports 40,000 system call handlers.

To learn how to create and customize call handlers, see the “Managing Call Handlers in Cisco Unity Connection 10.x” chapter.

# Directory Handlers in Cisco Unity Connection 10.x

Directory handlers provide access to a corporate directory that callers can use to reach Cisco Unity Connection users who have mailboxes and who are listed in the directory. When a caller searches for a username or part of a name, a directory handler looks up the extension and routes the call to the appropriate user. Callers can also enter an extension to place a call from a directory handler; the extension is checked against the applicable outcalling restriction table if the caller is a user, or against the Default Outdial restriction table if the caller is an outside caller.

There are two types of directory handlers:

| | |
|---|---|
| **Phone Keypad** | Callers enter search information or extensions by using the phone keypad. For this type of directory handler, you can specify how it searches for names, what it does when it finds one or more matches, and what it does when it detects no caller input. |
| **Voice Enabled** | *(For Cisco Unity Connection systems with the voice-recognition option only).* For this type of directory handler, callers say the first name and last name of the Unity Connection user that they want to reach, or enter an extension by saying the individual digits in the extension. In addition to searching by first and last name, the voice directory handler includes alternate names in searches. Callers can narrow down the search by saying the name and city or department of the user (or both) if these fields are defined on the **Edit User Basics** page in the user profile.<br><br>Unity Connection users who are listed in the directory are available to outside callers as names that can be reached. Administrator-defined contacts are only available to Unity Connection users who are signed in to Unity Connection, and user-defined contacts are only available to the Unity Connection users who defined them.<br><br>**Note** For this type of directory handler, users cannot be accessed by using directory handlers unless they have a display name specified and the List in Directory check box is checked for them on the **User Basics** page. |

To learn how to create and customize directory handlers, see the "Managing Directory Handlers in Cisco Unity Connection 10.x" chapter.

# Interview Handlers in Cisco Unity Connection 10.x

Interview handlers collect information from callers by playing a series of questions that you have recorded, and then recording the answers offered by callers. For example, you might use an interview handler to take sales orders or to gather information for a product support line.

When a call is routed to an interview handler, the interview handler plays the first recorded question, then plays a beep, then records the answer. Cisco Unity Connection stops recording either when the response reaches the maximum recording time that you have specified, or when the caller stops speaking. Unity Connection then plays the second question, and so on. When all the answers have been recorded, they are forwarded as a single voice message, with beeps separating the answers, to the recipient that you designate.

To learn how to create and customize interview handlers, see the "Managing Interview Handlers in Cisco Unity Connection 10.x" chapter.

# Call Routing Tables in Cisco Unity Connection 10.x

Call routing tables are used to route incoming calls to the operator or to specific users, call handlers, directory handlers, or interview handlers. In addition, call routing tables are used to route users to the user sign-in conversation.

Cisco Unity Connection has two call routing tables—one for direct calls and one for forwarded calls—that handle calls from users and from outside callers. Each table contains predefined routing rules, and you can create additional rules to route calls as needed. Set up your directory handlers, call handlers, and interview handlers first, and then modify or create call routing rules for each table as needed to route incoming calls correctly.

| | |
|---|---|
| **Direct Rules** | Direct rules handle calls from users and outside callers that are dialed directly to Unity Connection. The predefined direct routing rules are:<br>• Attempt Sign-In—Calls from users are routed to the user sign-in conversation.<br>• Opening Greeting—Calls from outside callers are routed to the Opening Greeting. |
| **Forwarded Rules** | Forwarded rules handle calls that are forwarded to Unity Connection from either a user extension or from an extension that is not associated with a user account (such as a conference room). The predefined forwarded routing rules are:<br>• Attempt Forward—All calls forwarded from a user extension are routed to the user greeting.<br>• Opening Greeting—Calls forwarded from an extension that is not associated with a user account are routed to the Opening Greeting. |

You can add new rules and change the order of the rules in the respective routing tables. You can change the order of the Attempt Sign-In and Attempt Forward rules relative to additional rules that you add in the respective routing tables, but the Opening Greeting rule is always the last entry for both tables. You cannot delete the predefined rules.

Review the following "How Call Routing Rules Work" section and the "Using Routing Rules with the Route from Next Call Routing Rule Action" section on page 4-6 to learn more about routing rules. When you are ready to create and customize them, see the "Managing Call Routing Tables in Cisco Unity Connection 10.x" chapter.

## How Call Routing Rules Work

Call routing tables consist of a series of rules that let you route incoming calls based on the information that Cisco Unity Connection may have about a call, such as the calling phone number (ANI or caller ID), the trunk or port on which the call comes in, the dialed phone number (DNIS), the forwarding station, and the schedule.

When Unity Connection receives a call, it first determines if it is a direct or forwarded call based on the call information that is sent by the phone system, and then applies the applicable call routing table. If the call information matches all of the conditions for the first rule, the call is routed as specified in the

rule. If any of the conditions specified in the first rule are not met, the call information is then compared to the conditions of the second rule, and so on, until a rule is found that matches all the characteristics of the call.

The integration between the phone system and Unity Connection determines the information that is provided about a call (for example, call type, port, trunk, calling number, and dialed number). The schedule is determined by the date and time that the call is received.

To set up routing rules correctly, you need to know what information your integration provides. See the Call Information section in the Cisco Unity Connection integration guide for your phone system for this information (Unity Connection integration guides are available at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html).

The following examples show how call routing tables are used in Unity Connection to route calls.

#### Example 1

In Table 4-1, calls that meet the criteria specified in the Operator rule settings—any direct external call received while the Weekdays schedule is active—are transferred to the operator. Calls that do not meet this criteria are routed as specified by one of the other call routing rules in the table. In this case, any direct external calls received on the weekends are routed to the Opening Greeting, according to the Opening Greeting call routing rule.

*Table 4-1 Direct Calls Call Routing Table*

| Rule | Status | Dialed Number | Calling Number | Phone System | Port | Schedule | Send Call To |
|---|---|---|---|---|---|---|---|
| Operator | Active | Any | Any | Any | Any | Weekdays | Attempt transfer for operator |
| Attempt Sign-In | Active | Any | Any | Any | Any | Always | Attempt Sign-In |
| Opening Greeting | Active | Any | Any | Any | Any | Always | Attempt transfer for Opening Greeting |

#### Example 2

In Table 4-2, calls forwarded from specific extensions—1234 and 5678—are routed according to the Product Info and Customer Service rules, respectively. Calls that do not match the extension (or forwarding station) in either of the first two rules are routed according to the two remaining rules.

*Table 4-2 Forwarded Calls Call Routing Table*

| Rule | Status | Dialed Number | Calling Number | Forwarding Station | Phone System | Port | Schedule | Send Call To |
|---|---|---|---|---|---|---|---|---|
| Customer Service | Active | Any | Any | 5678 | Any | Any | Always | Attempt transfer for Customer Service |
| Product Info | Active | Any | Any | 1234 | Any | Any | Always | Send to greeting for Product Info |
| Attempt Forward | Active | Any | Any | Any | Any | Any | Always | Attempt Forward |
| Opening Greeting | Active | Any | Any | Any | Any | Any | Always | Attempt transfer for Opening Greeting |

## Using Routing Rules with the Route from Next Call Routing Rule Action

In a user profile or call handler, you can configure the After Greeting action, the After Message action, or the action of a caller input key to apply the Route from Next Call Routing Rule action to calls. This action causes Cisco Unity Connection to continue processing the call according to the applicable call routing table (direct or forwarded, depending on how the call was received from the phone system) starting at the rule immediately after the rule that Unity Connection previously applied to the call. If the call was already processed according to the final rule in the table, the final rule is applied again.

For example, you might want to have Unity Connection always play a standard greeting or legal disclaimer to all callers, whether they call Unity Connection directly or are forwarded by an extension. The greeting plays before callers can take any other action—for example, leaving a message or signing in. To do so, you do the following tasks:

1. Create a new call handler and record the message as the alternate greeting.
2. Enable the alternate greeting, configure it to ignore caller input during the greeting, and then configure the After Greeting action with the Route from Next Call Routing Rule call action.
3. Add a new direct call routing rule to send all direct calls to the new call handler (with Go Directly to Greetings selected) and verify that the rule appears at the top of the direct call routing table.
4. Add a new forwarded call routing rule to send all forwarded calls to the same new call handler (again with Go Directly to Greetings selected) and verify that the rule appears at the top of the forwarded call routing table.

Once the system is configured in this way, all calls—no matter where they come from or how they get to the system—hear this greeting in its entirety and then proceed directly to their original destination.

# Restriction Tables in Cisco Unity Connection 10.x

Restriction tables allow you to control which phone numbers users and administrators can use for:

- Transferring calls—including both the numbers users can enter for transferring their calls, and the numbers that outside callers can enter when using Caller system transfers. (For more information on Caller system transfers, see the "System Transfer Overview in Cisco Unity Connection 10.x" section on page 14-1.)
- Recording and playback by phone from Cisco Unity Connection applications, when the phone is the designated recording and playback device in the Media Master.
- Delivering faxes to a fax machine.
- Sending message notifications.
- Creating user-defined alternate extensions—including the extensions that Unity Connection offers to add automatically on behalf of users.

For example, you can specify that users have calls transferred only to internal extensions or that faxes are delivered only to local phone numbers. (Restriction tables do not affect the phone numbers that users can dial directly from their phones when they are not interacting with Unity Connection.)

Each class of service specifies for its members a restriction table for call transfers, one for message notification, and one for fax deliveries. The restriction table can be the same for all three, or different for each.

Review the following "How Restriction Tables Work" section to learn more about restriction tables. When you are ready to create and customize them, see the "Managing Restriction Tables in Cisco Unity Connection 10.x" chapter.

# How Restriction Tables Work

When a user uses the Cisco Unity Connection Messaging Assistant or the Unity Connection conversation to attempt to change a phone number that is used for call transfer, message notification, or fax delivery, or when signed-in users use the Unity Connection conversation to perform User system transfers to a number that they specify, Unity Connection applies the restriction table associated with the class of service of the user to verify that the phone number entered is allowed.

For example, if a user uses the Unity Connection Messaging Assistant to enter a phone number to set up a message notification device, Unity Connection applies the restriction table that is associated with the class of service of that user, and displays an error message if the phone number is not allowed. But when an administrator changes a message notification number for a user by using Cisco Unity Connection Administration, Unity Connection does not apply any restriction table to the number. Therefore, an administrator can, when necessary, override the limitations of the class of service of a particular user.

The User-Defined and Automatically-Added Alternate Extensions restriction table functions similarly to other restriction tables in that it restricts the numbers the users can use to create alternate extensions for themselves through interfaces such as the Cisco Personal Communications Assistant or via an API call. It can also restrict a number from being offered as an alternate extension when a user frequently calls Unity Connection and signs in from the number. (The table is named Excluded Extensions for Automatically-Added Alternate Extensions, and does not apply to alternate extensions that users create for themselves in Cisco PCA.) Unlike other restriction tables, this restriction table applies to all users and therefore is not associated with a class of service. It also applies when administrators use Connection Administration to change user-defined alternate extensions, but does not apply when administrators enter or change administrator-defined alternate extensions.

Each row of a restriction table is made up of a dial string. Each dial string consists of a call pattern and a setting that specifies whether numbers that match the call pattern can be called. In most cases, the restriction table is applied when a user attempts to change a number that is controlled by a restriction table, not when Unity Connection tries to complete a transfer or delivery. In the case of Caller system transfers, which allow unauthenticated callers to transfer to a number that they specify, Unity Connection checks the specified number against the Default System Transfer table. By default, this table blocks all numbers, in order to protect against toll fraud and unauthorized use.

When a restriction table is applied to a number (such as a pager number for a message notification), Unity Connection compares the number with the call pattern of the first dial string in the restriction table. If the number does not match the call pattern, Unity Connection then compares the number with the call pattern in the second dial string, and so on, until it finds a match. When Unity Connection finds a match, it either permits or restricts calling the number as specified in the dial string.

Restriction tables are commonly used to permit or restrict calls to the following:

- Specific numbers, such as an extension.
- Numbers that are greater than or less than a specific length.
- Numbers that contain a specific digit or pattern of digits, such as an external access code followed by a long-distance access code.

For example, the restriction table in Table 4-3 restricts most long distance phone numbers, but permits extensions starting with “91.” In this case, if a user enters “9123” as a transfer number, Unity Connection first compares the number to the call pattern in Dial String 0, which restricts all numbers that begin with “91” and are followed by at least seven digits. Because the number entered does not match the call pattern, Unity Connection then compares the number to Dial String 1, which restricts all numbers that begin with “9011” and are followed by at least seven digits. Finally, Unity Connection compares the number to the last dial string, which contains the wildcard character that matches all numbers of any length. Because the Allow This String field is set to Yes for this dial string, Unity Connection permits this number to be used.

*Table 4-3 Example 1*

| Dial String | Call Pattern | Allow This String |
|---|---|---|
| 0 | 91???????* | No |
| 1 | 9011???????* | No |
| 2 | * | Yes |

The restriction table in Table 4-4 restricts long distance phone numbers and numbers with fewer than four digits. In this example, “9” is the external access code for the phone system, and “1” is the long-distance access code. Dial String 0 restricts any number beginning with “91,” while numbers fewer than four digits in length are restricted by Dial String 2. Thus, the only numbers permitted by this restriction table have at least four digits, and are not long distance phone numbers.

*Table 4-4 Example 2*

| Dial String | Call Pattern | Allow This String |
|---|---|---|
| 0 | 91* | No |
| 1 | ????* | Yes |
| 2 | * | No |

# Schedules and Holidays in Cisco Unity Connection 10.x

Schedules (and associated sets of holidays) are one of the variables that Cisco Unity Connection uses to manage calls: call handler transfer rules can be varied based on a schedule and schedules can be applied to routing rules to change call routing patterns for different time periods. Schedules also affect when some user and call handler greetings play.

Unity Connection offers two predefined schedules: All Hours, and Weekdays, both of which can be modified. (By default, the Weekdays schedule is configured to observe standard hours from 8 a.m. through 5 p.m. Monday through Friday, and to observe the predefined Holidays schedule, which does not contain any dates or times.)

For each schedule that you create or modify, you can identify multiple ranges of hours and days that make up the standard and closed hours, and associate a holiday schedule that defines specific holiday dates and times:

| | |
|---|---|
| **Standard hours** | The hours and days that make up the normal business hours, when the organization is open. Standard hours can include multiple time ranges and different time ranges on different days. (For example, standard hours for an organization might be Monday through Friday from 8 a.m. to 12 p.m. and 1 p.m. to 5 p.m., to accommodate a lunch break, and Saturday from 9 a.m. to 1 p.m.)<br><br>Standard transfer rules are in effect during the days and time ranges you add to the standard schedule; standard user and call handler greetings play during standard hours. |

| | |
|---|---|
| **Closed hours** | The hours and days not identified as standard hours are considered nonbusiness hours, when the organization is closed.<br><br>Closed user and call handler transfer rules operate at all times not specified by the standard schedule—including holidays; closed user and call handler greetings play according to the closed schedule. |
| **Holidays** | When a Holiday setting is in effect, Unity Connection plays holiday greetings (if enabled) and observes closed hours transfer rules. You can set up several years of holidays at a time. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.<br><br>Closed user and call handler transfer rules operate at all times not specified by the standard schedule—including holidays; holiday greetings for users and call handlers also play during this time period. |

To modify predefined schedules or to create your own, see the "Managing Schedules and Holidays in Cisco Unity Connection 10.x" chapter.

# Default Cisco Unity Connection 10.x Automated Attendant Behavior

The following example uses the default Cisco Unity Connection automated attendant configuration to illustrate a call flow through various call management elements. It illustrates some of the default behavior you can expect if you have not changed the call management configuration after installing Unity Connection.

### An Outside Caller Calls Cisco Unity Connection During Business Hours

A caller who does not have a Unity Connection mailbox dials the main Unity Connection phone number at 9:00 a.m. on a Monday morning.

1. Information from the phone system indicates that the call is a direct call from an outside caller. Unity Connection checks the call routing rules for a rule that matches the call. The Direct routing rules table contains two entries: Attempt Sign In and Opening Greeting. For the Attempt Sign-In rule, Unity Connection attempts to match the caller phone number with the extension or alternate extension of a Unity Connection user. When this fails, Unity Connection tries the next routing rule, the Opening Greeting rule.
2. The Opening Greeting call routing rule matches any incoming call at any time of day. It is configured to attempt to route the call to the Opening Greeting call handler.
3. Unity Connection checks the transfer option settings for the Opening Greeting call handler. Because the call came in during the Weekdays active schedule, the standard transfer options apply. These specify to send the call to the greeting for this call handler. (Note that if the Opening Greeting call routing rule had been configured to send the call to the greeting for the Opening Greeting call handler rather than attempting to transfer to it, this step would be skipped).
4. Because the call came in during the Weekdays active schedule from a phone number that did not match an internal Unity Connection user, Unity Connection plays the standard greeting for the call handler: "Hello: Cisco Unity Connection Messaging System. From a touchtone phone you may dial an extension at any time. For a directory of extensions, press 4. Otherwise, please hold for an operator."

5. While the greeting plays, as the greeting indicates, the caller can enter digits to reach a user extension. The caller input settings on the Opening Greeting call handler also define several one-key dialing actions that can be taken—for example, when the caller presses key 4, Unity Connection is configured to send the call to the System Directory Handler if no other keys are pressed within the time configured to wait for additional digits.
6. If no digits are entered, Unity Connection proceeds with the after greeting action for the Standard greeting on this call handler, which is configured to attempt to transfer the call to the Operator call handler.
7. The Operator call handler is also configured for the Weekdays active schedule, and once again, Unity Connection checks the standard transfer options for the call handler, which specify to transfer to the call handler greeting. The greeting plays: “Sorry, the operator is not available.”
8. The after greeting action for this greeting directs Unity Connection to take a message. The message settings for this call handler specify that the Operator user receives the message, and that after the caller leaves the message, Unity Connection should hang up.

# Creating a Call Management Plan in Cisco Unity Connection 10.x

**Note** Careful planning for your system components—call handlers, interview handlers, directory handlers, and call routing tables—is key to setting them up efficiently. Creating a call management map is a way to document your plan.

**Note** Before beginning the steps in this chapter, make sure you understand each of the system components and call routing elements as described in the "Call Management Overview in Cisco Unity Connection 10.x" chapter.

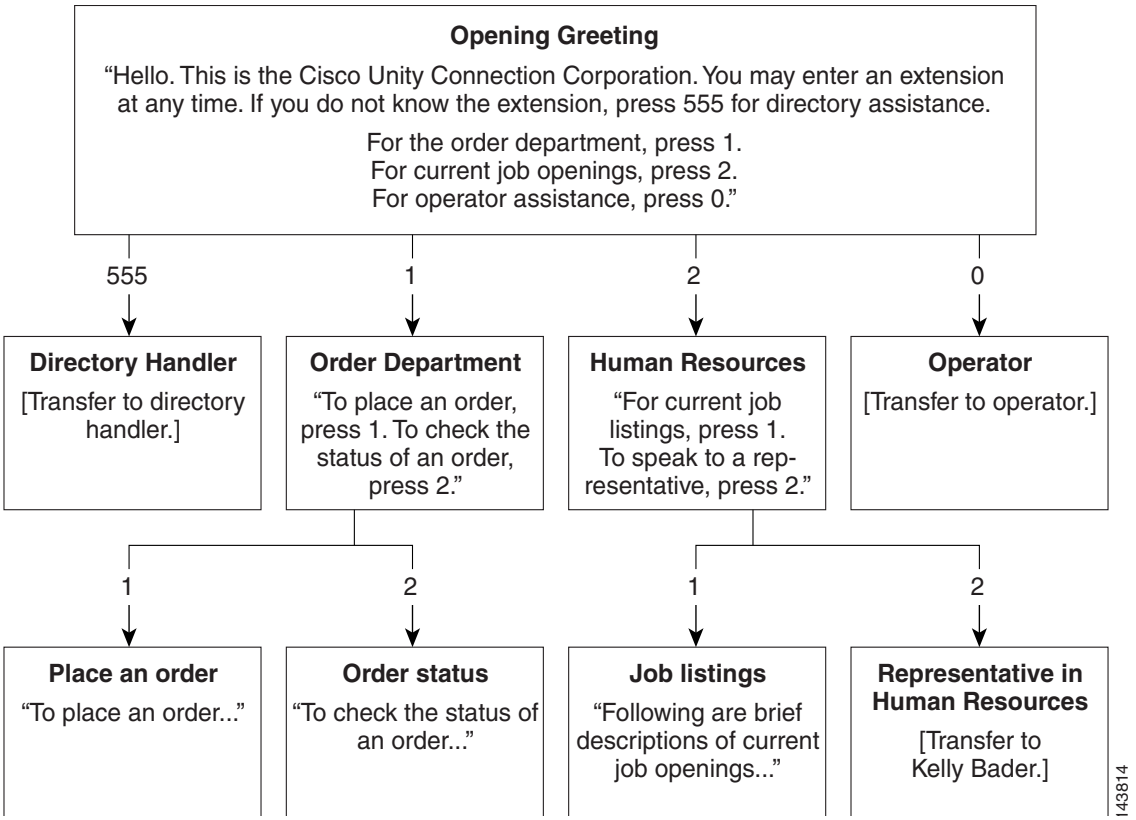
See the following sections:


- Creating a Call Management Map in Cisco Unity Connection 10.x, page 5-1
- Implementing a Call Management Plan in Cisco Unity Connection 10.x, page 5-2


## Creating a Call Management Map in Cisco Unity Connection 10.x

When you have considered how your call management plan ought to work, you can create a sketch that shows specifically how the handlers connect to one another. Include a menu of one-key dialing options and all possible navigation choices (such as reaching a call handler by dialing an extension or via a routing rule). You can also include the predefined Cisco Unity Connection call handlers in your plan. See Figure 5-1 for a sample call management map that makes use of the automated attendant.

*Figure 5-1 Sample Automated Attendant Call Management Map*




# Implementing a Call Management Plan in Cisco Unity Connection 10.x

After you have mapped your plan, write detailed scripts for the greeting of each call handler to use during the recording session.

When you are ready to set up your system of call handlers, start from the bottom up. First create the call handlers to which calls are routed. You select these "destination" call handlers when you create the call handlers that route calls to them. You also need to create accounts for the users to which call handlers transfer before creating those call handlers.

Using Figure 5-1 as an example, you first create a user account for Kelly Bader, and the handlers for Place an Order, Order Status, and Job Listings. Then you create the handlers for the Order Department and Human Resources.

In addition to mapping call handlers, you also need to plan call routing tables. In Figure 5-1, for example, all new call handlers are reached through the Opening Greeting. Another alternative is to assign extensions to some of your call handlers and to route incoming calls to those extensions by using a call routing table.

# Managing Call Handlers in Cisco Unity Connection 10.x

See the following sections:


- Overview of Default Call Handlers in Cisco Unity Connection 10.x, page 6-1
- Creating, Modifying, and Deleting Call Handler Templates in Cisco Unity Connection 10.x, page 6-2
- Creating Call Handlers in Cisco Unity Connection 10.x, page 6-4
- Modifying Call Handlers in Cisco Unity Connection 10.x, page 6-5
- Overview of Call Handler Greetings in Cisco Unity Connection 10.x, page 6-6
- Managing Call Handler Greetings in Cisco Unity Connection 10.x, page 6-8
- Managing Caller Input During Greetings in Cisco Unity Connection 10.x, page 6-9
- Changing Phone Language Settings in Cisco Unity Connection 10.x, page 6-12
- Taking Messages in Cisco Unity Connection 10.x, page 6-12
- Transferring Calls in Cisco Unity Connection 10.x, page 6-13
- Deleting Call Handlers in Cisco Unity Connection 10.x, page 6-13


## Overview of Default Call Handlers in Cisco Unity Connection 10.x

Cisco Unity Connection comes with the following predefined call handlers, which you can modify but not delete. Note that you should at least modify the greetings for these call handlers.

| | |
|---|---|
| **Opening Greeting** | Acts as an automated attendant, playing the greeting that callers first hear when they call your organization, and performing the actions you specify. The Opening Greeting Call Routing rule transfers all incoming calls to the Opening Greeting call handler.<br><br>By default, the Opening Greeting call handler allows callers to press * to reach the Sign-In conversation, or press # to reach the Operator call handler. Messages left in the Opening Greeting call handler are sent to the Undeliverable Messages distribution list. |

| | |
|---|---|
| **Operator** | Calls are routed to this call handler when callers press “0” or do not press any key (the default setting). You can configure the Operator call handler so that callers can leave a message or be transferred to a live operator.<br><br>By default, the Operator call handler allows callers to press * to reach the Sign-In conversation, or press # to reach the Opening Greeting call handler. Messages left in the Operator call handler are sent to the mailbox for the Operator user. |
| **Goodbye** | Plays a brief goodbye message and then hangs up if there is no caller input.<br><br>By default, the Goodbye call handler allows callers to press * to reach the Sign-In conversation, or press # to reach the Opening Greeting call handler. If you change the After Greeting action from Hang Up to Take Message, messages left in the Goodbye call handler are sent to the Undeliverable Messages distribution list. |

# Creating, Modifying, and Deleting Call Handler Templates in Cisco Unity Connection 10.x

Each call handler that you add in Cisco Unity Connection is based on a template. Settings from the template are applied as the call handler is created. Unity Connection comes with one default call handler template, which has settings that are suitable for most call handlers.

You can also create new templates.

Before you create call handlers, review the settings in the template that you plan to use and determine whether you need to make changes or create new templates. For each template, you should consider enabling the transfer, caller input, greetings, and message settings that will be needed for the call handlers that you plan to create. Note that if you change settings on a call handler template, the new settings are in effect only for new call handlers that are created by using that template. Changes to template settings do not affect existing call handlers.

Deleting a call handler template does not affect any call handlers that were based on that template when they were created. Note that you cannot delete the default template.

See the following procedures:

- To Create a Call Handler Template, page 6-2
- To Modify a Call Handler Template, page 6-3
- To Delete a Call Handler Template, page 6-4

### To Create a Call Handler Template

**Step 1** In Cisco Unity Connection Administration, expand **Templates**, then select **Call Handler Templates**.

**Step 2** On the **Search Call Handler Templates** page, select **Add New**.

**Step 3** On the **New Call Handler Template** page, enter basic settings, as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** On the **Edit Call Handler Template** page, continue entering applicable settings.

**Step 6** When you have finished entering settings on the **Edit Call Handler Template** page, select **Save**.

**Step 7** On the **Edit** menu, select any (or all) of the following related pages, to continue adding applicable settings to the new call handler template:

- Transfer Rules (see the "Transferring Calls in Cisco Unity Connection 10.x" section on page 6-13 for details)
- Caller Input (see the "Managing Caller Input During Greetings in Cisco Unity Connection 10.x" section on page 6-9 for details)
- Greetings (see the "Overview of Call Handler Greetings in Cisco Unity Connection 10.x" section on page 6-6 for details)
- Message Settings (see the "Taking Messages in Cisco Unity Connection 10.x" section on page 6-12 for details)

**Step 8** If you change any of the default settings on any of the pages listed in Step 7, select **Save** before leaving the page.

### To Modify a Call Handler Template

**Step 1** In Cisco Unity Connection Administration, expand **Templates**, then select **Call Handler Templates**.

**Step 2** On the **Search Call Handler Templates** page, select the display name of the call handler template that you want to modify.

**Note** If the call handler template that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler Template**, change settings, as applicable. (For field information, on the Help menu, select **This Page**.)

**Step 4** When you have finished changing settings on the **Edit Call Handler Template** page, select **Save**.

**Step 5** You may also want to change settings on any (or all) of the following related pages, as applicable:

- Transfer Rules (see the "Transferring Calls in Cisco Unity Connection 10.x" section on page 6-13 for details)
- Caller Input (see the "Managing Caller Input During Greetings in Cisco Unity Connection 10.x" section on page 6-9 for details)
- Greetings (see the "Overview of Call Handler Greetings in Cisco Unity Connection 10.x" section on page 6-6 for details)
- Message Settings (see the "Taking Messages in Cisco Unity Connection 10.x" section on page 6-12 for details)

**Step 6** If you change any of the settings on a page listed in Step 5, select **Save** before leaving the page.

### To Delete a Call Handler Template

**Step 1** In Cisco Unity Connection Administration, expand **Templates**, then select **Call Handler Templates**.

**Step 2** On the **Search Call Handler Templates** page, check the check box adjacent to the call handler template that you want to delete.

**Note** If the call handler template that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

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

**Step 4** Select **OK**.

# Creating Call Handlers in Cisco Unity Connection 10.x

After you have created or updated the templates that you plan to use, you are ready to create call handlers.

### To Create a Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, select **Add New**.

**Step 3** On the **New Call Handler** page, enter basic settings, as applicable. (For field information, on the Help menu, select **This Page**.)

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** On the **Edit Call Handler** page, continue entering settings for the call handler.

**Step 6** When you have finished entering settings on the **Edit Call Handler** page, select **Save**.

**Step 7** On the **Edit** menu, select any (or all) of the following related pages, to continue adding applicable settings to the new call handler:

- Transfer Rules (see the "Transferring Calls in Cisco Unity Connection 10.x" section on page 6-13 for details)
- Caller Input (see the "Managing Caller Input During Greetings in Cisco Unity Connection 10.x" section on page 6-9 for details)
- Greetings (see the "Overview of Call Handler Greetings in Cisco Unity Connection 10.x" section on page 6-6 for details)
- Message Settings (see the "Taking Messages in Cisco Unity Connection 10.x" section on page 6-12 for details)
- Call Handler Owners

**Note** Depending on how you set up the call handler template on which this new call handler is based, you may not need to change any settings on these additional pages. At a minimum, however, you should record a name and one or more greetings for the call handler.

**Step 8** If you change any of the settings on a page listed in Step 7, select **Save** before leaving the page.

# Modifying Call Handlers in Cisco Unity Connection 10.x

After a call handler has been created, you may need to adjust settings. The tools in Cisco Unity Connection Administration allow you to modify a single call handler at a time, or make changes to multiple call handlers at once. Do the applicable procedure:

- To Modify a Single Call Handler, page 6-5
- To Modify Call Handler Settings in Bulk Edit Mode, page 6-6

### To Modify a Single Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, select the display name of the call handler that you want to modify.

**Note** If the call handler that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler** page, change settings as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Note** Do remember to take backup of the report data before renaming the Call Handler display name as you will be unable to view the prior data set for calls in the report after renaming it.

**Step 4** When you have finished changing settings on the **Edit Call Handler** page, select **Save**.

**Step 5** You may also want to change settings on any (or all) of the following related pages, as applicable:

- Transfer Rules (see the "Transferring Calls in Cisco Unity Connection 10.x" section on page 6-13 for details)
- Caller Input (see the "Managing Caller Input During Greetings in Cisco Unity Connection 10.x" section on page 6-9 for details)
- Greetings (see the "Overview of Call Handler Greetings in Cisco Unity Connection 10.x" section on page 6-6 for details)
- Message Settings (see the "Taking Messages in Cisco Unity Connection 10.x" section on page 6-12 for details)
- Call Handler Owners

**Step 6** If you change any of the settings on a page listed in Step 5, select **Save** before leaving the page.

### To Modify Call Handler Settings in Bulk Edit Mode

**Step 1** On the **Search Call Handlers** page, check the applicable call handler check boxes, and select **Bulk Edit**.

If the call handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable call handlers. Then select **Bulk Edit**.

**Step 2** To make a change to a setting, check the check box to the left of the field name to select it, and then set the field as usual. Select **Help > This Page** to see descriptions of each setting.

**Note** The **Status** message at the top of the **Edit Call Handler Basics** page tells you how many call handlers are being edited. Also note that the page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 4** Select **Submit**.

# Overview of Call Handler Greetings in Cisco Unity Connection 10.x

Each call handler can have up to seven greetings. The greeting settings specify which greetings are enabled, how long they are enabled, the greeting source, and the actions that Cisco Unity Connection takes during and after each greeting. When a greeting is enabled, Unity Connection plays the greeting in the applicable situation until the specified date and time arrives, and then the greeting is automatically disabled. A greeting can also be enabled to play indefinitely.

**Note** Call Handler greetings can be recorded in multiple languages. See the "Changing Phone Language Settings in Cisco Unity Connection 10.x" section on page 6-12 for instructions.

You can customize how Unity Connection handles calls to call handlers that have the alternate greeting enabled. For example, you can specify that for as long as the alternate greeting is enabled, Unity Connection:

- Transfers callers directly to the greeting without ringing the extension that is assigned to the call handler (as applicable) whenever calls are transferred from the automated attendant or a directory handler to the user extension. (The phone rings if an outside caller or another Unity Connection user dials a user extension directly.)
- Prevents all callers from skipping the greeting.
- Prevents all callers from leaving messages (when the call handler is set up to take message).

**Note** Unity Connection plays the greetings that you enable for the applicable situation; however, some greetings override other greetings when they are enabled:

| | |
|---|---|
| **Standard** | Plays at all times unless overridden by another greeting. You cannot disable the standard greeting. |
| **Closed** | Plays during the closed (nonbusiness) hours defined for the active schedule. A closed greeting overrides the standard greeting, and thus limits the standard greeting to the open hours defined for the active schedule. |
| **Holiday** | Plays during the specific dates and times specified in the schedule of holidays associated with the active schedule. A holiday greeting overrides the standard and closed greetings. |
| **Internal** | Plays to internal callers only. It can provide information that only coworkers need to know. (For example, "I will be in the lab all afternoon.") An internal greeting overrides the standard, closed, and holiday greetings.<br>Not all phone system integrations provide the support necessary for an internal greeting. |
| **Busy** | Plays when the extension is busy. (For example, "All of our operators are with other customers.") A busy greeting overrides the standard, closed, internal, and holiday greetings.<br>Not all phone system integrations provide the support necessary for a busy greeting. |
| **Alternate** | Can be used for a variety of special situations, such as vacations or a leave of absence. (For example, "I will be out of the office until....") An alternate greeting overrides all other greetings. |
| **Error** | Plays if the caller enters invalid digits. This can happen if the digits do not match an extension, the extension is not found in the search scope, or the caller is otherwise restricted from dialing the digits. You cannot disable the error greeting.<br>The system default error recording is, "I did not recognize that as a valid entry." By default, after the error greeting plays, Unity Connection replays the greeting that was playing when the caller entered the invalid digits. |

Call handler owners can select a different call handler greeting or record the call handler greetings from the **System Call Handlers > Greetings** page in Cisco Unity Connection Administration, or they can use the Cisco Unity Greetings Administrator to do so by phone. (For more information on recording greetings and using the Cisco Unity Greetings Administrator, see the "Managing Recorded Greetings and Recorded Names in Cisco Unity Connection 10.x" chapter.)

See the following "Managing Call Handler Greetings in Cisco Unity Connection 10.x" section for instructions on changing call handler greeting settings.

# Managing Call Handler Greetings in Cisco Unity Connection 10.x

You can modify call handlers greetings by using Cisco Unity Connection Administration, or by calling Cisco Unity Connection by phone. When you use Connection Administration to modify greetings, you can do so for a single call handler, or you can modify the greetings for multiple call handlers at once.

Do the applicable procedure:

- To Set Up Call Handler Greetings for a Single Call Handler, page 6-8
- To Set Up Call Handler Greetings for Multiple Call Handlers in Bulk Edit Mode, page 6-8

To manage call handler greetings when you—or the call handler owners that you assign—cannot access Cisco Unity Connection Administration, you can use the Cisco Unity Greetings Administrator by phone. For more information, see the "Setting Up the 10.x Cisco Unity Greetings Administrator" section on page 20-4 and the "Using the 10.x Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings" section on page 20-2.

### To Set Up Call Handler Greetings for a Single Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, select the display name of the applicable call handler.

**Note** If the call handler does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit** menu, select **Greetings**.

**Step 4** On the **Greetings** page, select the display name of the greeting that you want to set up.

**Step 5** On the **Edit Greeting** page, enter settings as applicable.

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

**Step 7** To set up another greeting for the call handler, repeat Step 3 through Step 6.

### To Set Up Call Handler Greetings for Multiple Call Handlers in Bulk Edit Mode

**Step 1** On the **Search Call Handlers** page, check the applicable call handler check boxes, and select **Bulk Edit**.

If the call handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable call handlers. Then select **Bulk Edit**.

**Note** The **Status** message at the top of the **Edit Call Handler Basics** page tells you how many call handlers are being edited. Also note that each page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 2** On the **Edit** menu, select **Greetings**.

**Step 3** On the **Greetings** page, select the display name of the greeting that you want to set up.

**Step 4** On the **Edit Greeting** page, change settings as applicable by checking the check box to the left of a field name to select it, and then setting the field as usual. (Select **Help > This Page** to see descriptions of each setting.)

**Step 5** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 6** Select **Submit**.

# Managing Caller Input During Greetings in Cisco Unity Connection 10.x

Caller input settings define actions that Cisco Unity Connection takes in response to phone keys pressed by callers during a call handler greeting. By using the settings on the Edit Greeting page for each individual greeting, you can specify on a per-greeting basis whether the greeting allows caller input and whether callers can perform transfers. Or, you can define caller input keys and options that apply to all of the call handler greetings by using the Caller Input page for the call handler.

See the following sections for details:

- Offering One-Key Dialing During Call Handler Greetings, page 6-9
- Offering System Transfers, page 6-10
- Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter, page 6-10

## Offering One-Key Dialing During Call Handler Greetings

One-key dialing enables you to designate a single digit to represent a user extension, alternate contact number, call handler, interview handler, or directory handler. Instead of entering the full extension, the caller presses a single key during a call handler greeting and Cisco Unity Connection responds accordingly. By specifying several different keys as caller input options, you can offer callers a menu of choices in the call handler greeting.

Configuring the transfer to alternate contact number action on one or more keys of a call handler allows you to quickly set up a simple audiotext tree that callers can use to transfer to specific non-user extensions on the phone system or to specific external numbers, without having to create separate call handlers for each number. When transferring a caller to an alternate contact number, Unity Connection can either supervise the transfer or release the call to the phone system.

Callers can also bypass one-key dialing. You set the system to pause a certain number of seconds for additional key presses before routing the call according to the one-key dialing menu you have set up. These pauses allow callers to press full extension IDs to bypass one-key dialing menus, even during the handler greeting.

Further, you can lock certain keys to take the caller directly to the action programmed for that key without waiting for an additional key press. Note that you should not lock any key that matches the first digit of user extensions; otherwise, callers are not able to enter an extension to reach a user.

### To Offer One-Key Dialing During a Call Handler Greeting

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handler** page, in the **Search Results** table, select the display name of the applicable call handler.

**Note** If the call handler does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler** page, on the **Edit** menu, select **Caller Input**.

**Step 4** In the **Single Key Settings** table, select the applicable phone keypad key.

**Step 5** On the **Edit Caller Input** page for the key that you selected, check the **Ignore Additional Input (Locked)** check box to instruct Unity Connection to immediately process the key without waiting for the caller to enter additional digits.

**Step 6** Under **Action**, select an option and change settings as applicable.

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

**Step 8** Optionally, you can rerecord the call handler greetings to mention the key that callers can press while listening to the greetings:

a. On the **Edit** menu, select **Greetings**.

b. On the **Greetings** page, select the display name of the greeting that you want to modify.

c. On the **Edit Greeting** page, select **Play/Record**, and record a greeting.

d. Select **Save**.

# Offering System Transfers

System transfers allow callers to dial numbers that are not associated with a user, contact, call handler, or other entity. For example, users and outside callers may find it convenient to be able to call Cisco Unity Connection and transfer from a call handler to a lobby extension, conference room extension, or an extension that is assigned to someone in the organization who is not a Unity Connection user, such as an employee who is visiting from another site and is using a guest office.

You can configure individual call handler greetings to allow callers to transfer to numbers that are not associated with Unity Connection users or call handlers while the greeting is playing.

For more information see the "Setting Up System Transfers in Cisco Unity Connection 10.x" chapter.

# Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter

You can simulate abbreviated extensions by using prepended digits for call handlers and user mailboxes. When such digits are defined, they are prepended to any extension that a caller dials while listening to the greeting for the call handler or user mailbox.

Cisco Unity Connection first attempts to route the call to the prepended extension. If the prepended extension is not valid, Unity Connection attempts to route the call to the dialed extension. In the following example, the call handler named Sales is configured with the prepended digits 123. When a caller dials 1000 while listening to the greeting for the Sales call handler, Unity Connection attempts to route the call to extension 1231000; if the prepended extension is not valid, Unity Connection attempts to route the call to extension 1000. (Note that if extension 1000 is not a valid extension and the greeting for the Sales call handler is configured to allow transfers to numbers not associated with users or call handlers, Unity Connection performs a release transfer to 1231000.)

Abbreviated extensions can be used as a way for an organization to segment users into different groups. For example, suppose a company has two departments: Engineering and Marketing. The company uses six digit extensions, and all extensions in Engineering begin with 10 and all extensions in Marketing begin with 11. Call handlers could be created for Engineering and for Marketing, and each call handler could be configured to prepend a 10 or a 11, as applicable, to any extension dialed from that call handler. When set up this way, users would only have to enter the last four digits of a user extension.

Do one of the following procedures:

- To Configure Prepended Digits for Individual User or Call Handler Accounts, page 6-11
- To Configure Prepended Digits for Multiple User or Call Handler Accounts in Bulk Edit Mode, page 6-11

#### To Configure Prepended Digits for Individual User or Call Handler Accounts

**Step 1** In Cisco Unity Connection Administration, go to the **Caller Input** page for the applicable user, user template, call handler, or call handler template.

**Step 2** In the **Prepend Digits to Dialed Extensions** section, check the **Enable** check box.

**Step 3** In the **Digits to Prepend** field, enter the applicable digits.

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

#### To Configure Prepended Digits for Multiple User or Call Handler Accounts in Bulk Edit Mode

**Step 1** On the applicable **Search** page, check the applicable user or call handler check boxes, and select **Bulk Edit**.

If the users or call handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable users or call handlers. Then select **Bulk Edit**.

**Note** The **Status** message at the top of the page tells you how many users or call handlers are being edited. Also note that each page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 2** On the **Edit** menu, select **Caller Input**.

**Step 3** On the **Caller Input** page, in the **Prepend Digits to Dialed Extensions** section, check the left-most check box to select the **Enable** field, and then check the **Enable** check box.

**Step 4** In the **Digits to Prepend** field, enter the applicable digits.

**Step 5** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 6** Select **Submit**.

# Changing Phone Language Settings in Cisco Unity Connection 10.x

Call handler greetings can be recorded in multiple languages when the language for the call handler is inherited from the caller. For example, if Cisco Unity Connection is configured to provide prompts in French and Spanish, it is possible to record the standard greeting in both languages so that Spanish- and French-speaking callers can hear the greeting in their own language.

### To Change Phone Language Settings for a Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handler** page, in the **Search Results** table, select the display name of the applicable call handler.

**Note** If the call handler does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler** page, select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the Language list.

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

**Step 5** On the **Edit** menu, select **Greetings**.

**Step 6** On the **Greetings** page, select the applicable greeting.

**Step 7** On the **Edit Greetings** page, rerecord greetings in the new language.

**Step 8** Select **Save**.

# Taking Messages in Cisco Unity Connection 10.x

By using the settings for a particular call handler greeting, you can configure the call handler to take a message after playing the greeting. You can specify who receives messages for the call handler, whether messages are marked for dispatch delivery, the maximum recording length for messages from outside callers, what callers can do when leaving messages and whether their messages are automatically marked secure, and what action to take next on a call after a message is left.

Note that for some integrations, you can set up Cisco Unity Connection so that as a caller records a message, a warning prompt is played before the caller reaches the maximum allowable message length. See the "Configuring the Termination Warning Prompt for the End of Recording" section on page 22-6 for details.

For details on configuring dispatch messages, see the "Dispatch Messages in Cisco Unity Connection 10.x" section on page 22-8.

# Transferring Calls in Cisco Unity Connection 10.x

The call transfer settings for a call handler specify how Cisco Unity Connection transfers calls that reach the call handler from the automated attendant. Each call handler has three transfer rules that you can customize: one for standard hours and one for closed (nonbusiness and holiday) hours of the active schedule, and an alternate transfer rule that, when enabled, overrides the standard and closed transfer rules and is in effect at all times. When a call is transferred to the call handler, Unity Connection first checks the applicable transfer rule to determine where to transfer the call—either to the call handler greeting, or to an extension.

When transferring to the call handler greeting, Unity Connection plays the applicable greeting (standard, closed, holiday, internal, busy, or alternate) based on the situation and which greetings are enabled. You configure a transfer rule to transfer to the greeting if you want to use the call handler to provide the caller with a prerecorded menu of options or an informational message.

To route callers to a specific user or to another call handler, you configure the transfer rule to transfer to the extension of the user or call handler. When transferring a call to a user extension, Unity Connection can either release the call to the phone system, or it can supervise the transfer. When Unity Connection is set to supervise transfers, it can provide call screening and call holding options on indirect calls:

- With call screening, Unity Connection can ask for the name of the caller before connecting to a user. The user can then hear who is calling and, when a phone is shared by more than one user, who the call is for. The user can then accept or refuse the call.
- With call holding, when the phone is busy, Unity Connection can ask callers to hold. Each caller on hold uses a Unity Connection port and a phone system port, and therefore the total number of callers that can be holding in the queue at any one time is limited by the number of available ports.

  The default wait time in the call holding queue for the first caller in the queue is 25 seconds. If the caller is still on hold after this amount of time, Unity Connection asks whether the caller wants to continue holding, leave a message, or try another extension. In case of callers put on hold without asking, these options are available for the users after the first timeout of the default wait time. If the caller does not press a key on the phone keypad or say a voice command to indicate that he or she wants to continue holding, leave a message, or dial another extension, the caller is transferred back to the Opening Greeting. Subsequent callers in the holding queue are told how many other callers are in the queue ahead of them, in addition to these options. (See the "Call Holding Wait Time in Cisco Unity Connection 10.x" section on page 16-5 for more information on call holding.)

  If call holding is not selected, callers are sent to the user or handler greeting that is enabled: the standard, closed, holiday, busy, or alternate greeting.

# Deleting Call Handlers in Cisco Unity Connection 10.x

If a call handler is referenced by other objects in Unity Connection (for example, a routing rule or other call handler is set to route calls to the call handler), you are not allowed to delete the call handler until you have changed settings on the other objects to remove references to the call handler you want to delete. If you try to delete a call handler without first changing settings on objects that reference the call handler, the delete operation fails

If you delete call handlers that are referenced by other call handlers, be sure to rerecord the greetings so that callers hear the correct information about input options.

### To Delete a Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, check the check box adjacent to the display name of the call handler that you want to delete.

**Note** If the call handler that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** Select **Show Dependencies** to search for database objects that have dependencies on the call handler you want to delete.

**Step 4** From the dependencies search results, follow links to the affected objects and reassign the dependency to another call handler.

**Step 5** Select **Tools > Show Dependency Results**.

**Step 6** On the **Show Dependency Results** page, select **Display Previous Results**.

**Step 7** Repeat Step 4 through Step 6 until all dependencies have been reassigned.

**Step 8** Select **Call Management > System Call Handlers**.

**Step 9** On the **Search Call Handlers** page, check the check box adjacent to the display name of the call handler that you want to delete.

**Step 10** Select **Delete Selected**.

**Note** If you are concerned that you might delete the wrong call handler from the search page, you can select the display name to navigate to the **Edit Call Handler Basics** page. Use the detailed data on that page to confirm that it is the call handler you want to delete.

**Step 11** In the dialog box that asks you to confirm the deletion, select **OK**.

# Managing Directory Handlers in Cisco Unity Connection 10.x

**Note** Directory handlers provide access to a corporate directory that callers can use to reach Cisco Unity Connection users with mailboxes. When a caller searches for a username or part of a name, a directory handler looks up the extension and routes the call to the appropriate user.

Each directory handler contains settings that specify how it searches for names, what it does when it finds one or more matches, and what it does when it detects no caller input.

See the following sections:


- Overview of the Default Directory Handler in Cisco Unity Connection 10.x, page 7-1
- Creating a Directory Handler in Cisco Unity Connection 10.x, page 7-2
- Modifying a Directory Handler in Cisco Unity Connection 10.x, page 7-2
- Changing Phone Language Settings in Cisco Unity Connection 10.x, page 7-3
- Routing Calls to a Voice Directory Handler in Cisco Unity Connection 10.x, page 7-4
- Deleting a Directory Handler in Cisco Unity Connection 10.x, page 7-5


## Overview of the Default Directory Handler in Cisco Unity Connection 10.x

Cisco Unity Connection includes one default directory handler, the System Directory Handler, which you can modify but not delete. By default, this directory handler is configured to search all users who have mailboxes on the system, in last name, first name order. Callers use the phone keypad to interact with the default System Directory Handler. There is no default voice-enabled directory handler. (For additional discussion of the types of directory handlers, see the "Directory Handlers in Cisco Unity Connection 10.x" section on page 4-3.)

In the default configuration, the default directory handler is accessed when callers press 4 during the Opening Greeting call handler greeting.

# Creating a Directory Handler in Cisco Unity Connection 10.x

You can create as many directory handlers as needed to route calls to users by using available filters such as location and search space. You can create both phone-keypad and voice-enabled directory handlers on the same system, and users can be listed in more than one directory handler.

**Note** The voice-recognition option is required in order to create voice-enabled directory handlers.

Because directory handlers do not have greetings, we recommend that you use call handlers or one-key dialing to route callers to a directory handler, and use the call handler greeting to explain caller options for each directory handler.

By creating more than one directory handler, you can provide efficient and secure directory searches for systems with hundreds or thousands of users. Multiple directory handlers can also be used for call routing in headquarters and branch office deployments where Cisco Unity Connection provides centralized call processing. Users can be listed in more than one directory handler, and you can create as many directory handlers as needed to manage caller searches for users.

### To Create a Directory Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Directory Handlers**.

**Step 2** On the **Search Directory Handlers** page, select **Add New**.

**Step 3** On the **New Directory Handler** page, enter a display name and, optionally, an extension for the directory handler.

**Note** Fields marked with * (an asterisk) are required.

**Step 4** To create a voice-enabled directory handler, check the **Voice Enabled** check box.

**Step 5** Select **Save**.

**Step 6** On the **Edit Directory Handler Basics** page, continue entering settings for the directory handler. (For field information, on the **Help** menu, select **This Page**.)

**Step 7** When you have finished entering settings on the **Edit Directory Handler** page, select **Save**.

**Step 8** On the **Edit** menu, select **Caller Input** to continue adding applicable settings to the new directory handler.

**Step 9** If you change any of the settings on the **Caller Input** page, select **Save** before leaving the page.

# Modifying a Directory Handler in Cisco Unity Connection 10.x

Do the applicable procedure:

- To Modify a Directory Handler, page 7-3
- To Modify Directory Handler Settings in Bulk Edit Mode, page 7-3

### To Modify a Directory Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Directory Handlers**.

**Step 2** On the **Search Directory Handlers** page, select the display name of the directory handler that you want to modify.

**Note** If the directory handler that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Directory Handler Basics** page, change settings as applicable. (For field information, on the Help menu, select **This Page**.)

**Step 4** When you have finished changing settings on the **Edit Directory Handler** page, select **Save**.

**Step 5** To change the settings on the **Caller Input** page, on the **Edit** menu, select **Caller Input**.

**Step 6** If you change any of the settings on the **Caller Input** page, select **Save** before leaving the page.

### To Modify Directory Handler Settings in Bulk Edit Mode

**Step 1** On the **Search Directory Handlers** page, check the applicable directory handler check boxes, and select **Bulk Edit**.

If the directory handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable directory handlers. Then select **Bulk Edit**.

**Step 2** To make a change to a setting, check the check box to the left of the field name to select it, and then set the field as usual. Select **Help > This Page** to see descriptions of each setting.

**Note** The **Status** message at the top of the **Edit Directory Handler Basics** page tells you how many directory handlers are being edited. Also note that the page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the Bulk Edit operation for a later date and/or time.

**Step 4** Select **Submit**.

# Changing Phone Language Settings in Cisco Unity Connection 10.x

For each phone directory handler, you can specify whether to use the language that was applied by a previous call handler or by a routing rule.

Do the applicable procedure:

- To Change Phone Language Settings for a Directory Handler, page 7-4
- To Change Phone Language Settings for Multiple Directory Handlers in Bulk Edit Mode, page 7-4

#### To Change Phone Language Settings for a Directory Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Directory Handlers**.

**Step 2** On the **Search Directory Handlers** page, select the directory handler display name.

**Note** If the directory handler does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Directory Handler Basics** page, select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.

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

#### To Change Phone Language Settings for Multiple Directory Handlers in Bulk Edit Mode

**Step 1** On the **Search Directory Handlers** page, check the applicable directory handler check boxes, and select **Bulk Edit**.

If the directory handlers that you want to edit in bulk do not all appear on one Search page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable directory handlers. Then select **Bulk Edit**.

**Step 2** On the **Edit Directory Handler Basics** page, check the **Language** check box to select it, and then select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 4** Select **Submit**.

# Routing Calls to a Voice Directory Handler in Cisco Unity Connection 10.x

Because directory handlers do not have greetings, we recommend that you use call handlers or one-key dialing to route callers to a directory handler, and use the call handler greeting to explain caller options for each directory handler.

If you are setting up a voice directory handler, see the following task list for configuring Cisco Unified Communications Manager to route a phone number from Cisco Unified CM to the Cisco Unity Connection voice directory.

### Task List for Routing Calls to the Voice Directory Handler

1. In Cisco Unified CM Administration, add the ports that you want to use for the voice-type directory handler to a new line group.
2. Add the line group to a new hunt list.

3. Add the hunt list to a new hunt pilot to which calls for the voice-type directory handler will be routed.
4. In Cisco Unity Connection Administration, configure the ports to route calls to the voice-type directory handler.

For details on configuring Cisco Unified CM, see the Cisco Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

# Deleting a Directory Handler in Cisco Unity Connection 10.x

If a directory handler is referenced by other objects in Unity Connection (for example, a routing rule or a system call handler is set to route calls to the directory handler), you are not allowed to delete the directory handler until you have changed settings on the other objects to remove references to the directory handler you want to delete. If you try to delete a directory handler without first changing settings on objects that reference the directory handler, the delete operation fails

If you delete a directory handler that was referenced by one or more call handlers, be sure to rerecord the call handler greetings so that callers hear the appropriate information about input options.

### To Delete a Directory Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Directory Handlers**.

**Step 2** On the **Search Directory Handlers** page, select the check box adjacent to the display name of the directory handler that you want to delete.

**Note** If the directory handler that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** Select **Show Dependencies** to search for database objects that have dependencies on the directory handler you want to delete.

**Step 4** From the dependencies search results, follow links to the affected objects and reassign the dependency to another directory handler.

**Step 5** Select **Tools > Show Dependency Results**.

**Step 6** On the Show Dependency Results page, select **Display Previous Results**.

**Step 7** Repeat Step 4 through Step 6 until all dependencies have been reassigned.

**Step 8** Select **Call Management > Directory Handlers**.

**Step 9** On the **Search Directory Handlers** page, check the check box adjacent to the display name of the directory handler that you want to delete. Select **Delete Selected**.

**Note** If you are concerned that you might delete the wrong directory handler from the search page, select the display name to navigate to the Edit Directory Handler Basics page. Use the data on that page to confirm that it is the directory handler you want to delete.

**Step 10** In the dialog box that asks you to confirm the deletion, select **OK**.

# Managing Interview Handlers in Cisco Unity Connection 10.x

Interview handlers collect information from callers by playing a series of questions that you have recorded, and then recording the answers offered by callers. For example, you might use an interview handler to take sales orders or to gather information for a product support line.

You can specify who receives the messages for the interview handler, whether the message is marked for dispatch delivery, whether the message is marked urgent, and what action to take next on the call after a message is left.

See the following sections:


- Creating Interview Handlers in Cisco Unity Connection 10.x, page 8-1
- Modifying Interview Handlers in Cisco Unity Connection 10.x, page 8-2
- Changing Phone Language Settings in Cisco Unity Connection 10.x, page 8-3
- Deleting Interview Handlers in Cisco Unity Connection 10.x, page 8-4


## Creating Interview Handlers in Cisco Unity Connection 10.x

### To Create an Interview Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Interview Handlers**.

**Step 2** On the **Search Interview Handlers** page, select **Add New**.

**Step 3** On the **New Interview Handler** page, enter basic settings, as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** On the **Edit Interview Handler** page, on the **Edit** menu, select **Interview Questions**.

**Step 6** On the Interview Questions page, select a question number to configure settings and record audio for each question.

**Step 7** If you change any of the default settings on any of the questions, select **Save** before leaving the page.

# Modifying Interview Handlers in Cisco Unity Connection 10.x

Do the applicable procedure:

- To Modify an Interview Handler, page 8-2
- To Modify Interview Handler Settings in Bulk Edit Mode, page 8-2

### To Modify an Interview Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Interview Handlers**.

**Step 2** On the **Search Interview Handlers** page, select the display name of the interview handler that you want to modify.

**Note** If the interview handler that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Interview Handler** page, change settings, as applicable. (For field information, on the Help menu, select **This Page**.)

**Step 4** When you have finished changing settings on the **Edit Interview Handler** page, select **Save**.

**Step 5** On the **Edit** menu, select **Interview Questions**.

**Step 6** On the **Interview Questions** page, select a question number to change settings for each question, as applicable.

**Step 7** If you change any of the default settings on any of the question pages, select **Save** before leaving the page.

### To Modify Interview Handler Settings in Bulk Edit Mode

**Step 1** On the **Search Interview Handlers** page, check the applicable interview handler check boxes, and select **Bulk Edit**.

If the interview handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable interview handlers. Then select **Bulk Edit**.

**Step 2** To make a change to a setting, check the check box to the left of the field name to select it, and then set the field as usual. Select **Help > This Page** to see descriptions of each setting.

**Note** The **Status** message at the top of the **Edit Interview Handler Basics** page tells you how many interview handlers are being edited. Also note that the page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 4** Select **Submit**.

# Changing Phone Language Settings in Cisco Unity Connection 10.x

Do the applicable procedure:

- To Change Phone Language Settings for an Interview Handler, page 8-3
- To Change Phone Language Settings for Multiple Interview Handlers in Bulk Edit Mode, page 8-3

### To Change Phone Language Settings for an Interview Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Interview Handlers**.

**Step 2** On the **Search Interview Handlers** page, select the interview handler display name.

**Note** If the interview handler does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Interview Handler Basics** page, select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.

**Step 4** If applicable, rerecord questions in the new language:

a. On the **Edit** menu, select **Interview Questions**.

b. On the **Interview Questions** page, select a question number.

c. On the **Edit Interview Question** page, rerecord the question.

**Step 5** As you make changes on the pages, select **Save** before leaving a page.

### To Change Phone Language Settings for Multiple Interview Handlers in Bulk Edit Mode

**Step 1** On the **Search Interview Handlers** page, check the applicable interview handler check boxes, and select **Bulk Edit**.

If the interview handlers that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable interview handlers. Then select **Bulk Edit**.

**Step 2** On the **Edit Interview Handler Basics** page, check the **Language** check box to select it, and then select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 4** Select **Submit**.

# Deleting Interview Handlers in Cisco Unity Connection 10.x

If an interview handler is referenced by other objects in Unity Connection (for example, a caller input key on a call handler sends calls to the interview handler), you are not allowed to delete the interview handler until you have changed settings on the other objects to remove references to the interview handler you want to delete. If you try to delete a interview handler without first changing settings on objects that reference the interview handler, the delete operation fails

If you delete an interview handler that was referenced by one or more call handlers, be sure to rerecord the call handler greetings so that callers hear the appropriate information about input options.

### To Delete an Interview Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Interview Handlers**.

**Step 2** On the **Search Interview Handlers** page, check the check box adjacent to the display name of the interview handler that you want to delete.

**Note** If the interview handler that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** Select **Show Dependencies** to search for database objects that have dependencies on the interview handler you want to delete.

**Step 4** From the dependencies search results, follow links to the affected objects and reassign the dependency to another interview handler.

**Step 5** Select **Tools > Show Dependency Results**.

**Step 6** On the **Show Dependency Results** page, select **Display Previous Results**.

**Step 7** Repeat Step 4 through Step 6 until all dependencies have been reassigned.

**Step 8** Select **Call Management > Interview Handlers**.

**Step 9** On the **Search Interview Handlers** page, check the check box adjacent to the display name of the interview handler that you want to delete.

**Step 10** Select **Delete Selected**.

**Note** If you are concerned that you might delete the wrong interview handler from the search page, select the display name to navigate to the **Edit Interview Handler Basics** page. Use the data on the page to confirm that it is the interview handler you want to delete.

**Step 11** In the dialog box that asks you to confirm the deletion, select **OK**.

# Managing Custom Recordings in Cisco Unity Connection 10.x

See the following sections:


- Overview of the Custom Recordings in Cisco Unity Connection 10.x, page 9-1
- Adding a New Custom Recording in Cisco Unity Connection 10.x, page 9-2
- Modifying a Custom Recording in Cisco Unity Connection 10.x, page 9-2
- Setting After Message Sent Custom Recording in Cisco Unity Connection 10.x, page 9-3
- Deleting a Custom Recording in Cisco Unity Connection 10.x, page 9-5


## Overview of the Custom Recordings in Cisco Unity Connection 10.x

Cisco Unity Connection allows you to play the customized recordings after a message is sent. You can also play the custom recordings after a greeting is played. A greeting is played before the callers are allowed to leave a message for a user or a call handler.

**Note** In Cisco Unity Connection 10.0, the **Post Greeting Recordings** option is changed to the **Custom Recordings** option.

In Cisco Unity Connection Administration, after the message is sent, you have the options to play: no recording, default system recording, or custom recordings. Unity Connection allows you to add a new custom recording, modify the existing recording, and delete the existing recording. In addition, you can record multiple custom recordings in various languages that can be played after a message is sent and after a greeting is played.

To record each custom recording, you need to use the Media Master on the **Edit Custom Recording** page. The custom recordings are configured on the **Call Management > Custom Recordings** page in Cisco Unity Connection Administration. The **Play After Message Recording** and **Post Greeting Recording** options can be set for the following:

- Users
- User Templates
- Call Handlers

- Call Handler Templates

# Adding a New Custom Recording in Cisco Unity Connection 10.x

### To Add a new Custom Recording

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Custom Recordings**.

**Step 2** On the **Search Custom Recordings** page, select **Add New**.

**Step 3** On the **New Custom Recording** page, enter a display name for the custom recording.

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** On the **Edit Custom Recording** page, continue entering settings for the custom recording. (For field information, on the **Help** menu, select **This Page**.)

**Step 6** Select the language in which you want to record and select **Play/Record**.

**Step 7** When you are finished with the recording on the **Edit Custom Recordings** page, select **Save**.

### See Also

- New Custom Recording, page 6-39

# Modifying a Custom Recording in Cisco Unity Connection 10.x

### To Modify a Custom Recording

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Custom Recordings**.

**Step 2** On the **Search Custom Recordings** page, select the display name of the custom recording that you want to modify.

**Note** If the custom recording that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Custom Recording** page, change settings as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Step 4** When you finished changing settings on the **Edit Custom Recording** page, select **Save**.

**See Also**

- Edit Custom Recording, page 6-39

# Setting After Message Sent Custom Recording in Cisco Unity Connection 10.x

Do the applicable procedure:

- To Set After Message Sent Custom Recording for a User, page 9-3
- To Set After Message Set Custom Recording for a User Template, page 9-3
- To Set After Message Sent Custom Recording for a Call Handler Template, page 9-4
- To Set After Message Sent Custom Recording for a System Call Handler, page 9-4
- To Set After Message Sent Custom Recording for a User in Bulk Edit Mode, page 9-5

**Note** By default, **System Default Recording** option is selected for users, user templates, call handler templates, and system call handlers on the **Edit Message Settings** page.

### To Set After Message Sent Custom Recording for a User

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **users**.

**Step 2** On the **Search Users** page, select the user display name.

**Note** If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Users Basics** page, select **Message Settings** from the **Edit** menu.

**Step 4** On the **Edit Message Settings** page, select the **Play Recording** option, and then select the required recording from the **Recording Selection** drop-down list.

**Step 5** Select **Save**.

See Also

- Edit Message Settings, page 1-21

### To Set After Message Set Custom Recording for a User Template

**Step 1** In Cisco Unity Connection Administration, expand **Templates**, then select **User Templates**.

**Step 2** On the **Search User Templates** page, select the user template display name.

**Note** If the user template does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit User Templates Basics** page, select **Message Settings** from the **Edit** menu.

**Step 4** On the **Edit Message Settings** page, select the **Play Recording** option and then select the required recording from the **Recording Selection** drop-down list.

**Step 5** Select **Save**.

See Also

- User Templates Message Settings, page 3-14

#### To Set After Message Sent Custom Recording for a Call Handler Template

**Step 1** In Cisco Unity Connection Administration, expand **Templates**, then select **Call Handler Templates**.

**Step 2** On the **Search Call Handler Templates** page, select the call handler template display name.

**Note** If the call handler template does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler Templates Basics** page, select **Message Settings** from the **Edit** menu.

**Step 4** On the **Edit Message Settings** page, select the **Play Recording** option and then select the required recording from the **Recording Selection** drop-down list.

**Step 5** Select **Save**.

See Also

- Call Handler Templates Message Settings, page 3-73

#### To Set After Message Sent Custom Recording for a System Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers Templates** page, select the call handlers display name.

**Note** If the call handler template does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler Basics** page, select **Message Settings** from the **Edit** menu.

**Step 4** On the **Edit Message Settings** page, select the **Play Recording** option and then select the required recording from the **Recording Selection** drop-down list.

**Step 5** Select **Save**.

See Also

- Call Handler Message Settings, page 6-18

### To Set After Message Sent Custom Recording for a User in Bulk Edit Mode

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **users**.

**Step 2** On the **Search Users** page, check the applicable user check boxes, and select **Bulk Edit**.

If the users that you want to edit in bulk do not appear on one Search page, check all the applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all the applicable call handlers. Then select **Bulk Edit**.

**Step 3** On the **Edit User Basics** page, select **Message Settings** from the **Edit** menu.

**Step 4** On the **Edit Message Settings** page, check the check box to the left of the field name (**Play After Message Recording**) to select it, and then select the required recording from the **Recording Selection** drop-down list. Select **Help > This Page** to see descriptions of each setting.

**Note** The **Status** message at the top of the **Edit User Basics** page tells you how many users are being edited. Also note that the page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 5** Select **Submit**.

**Step 6** Repeat Step 1 to Step 5 to set the custom recordings for system call handlers in **Bulk Edit** mode.

See Also

- Custom Recordings in Cisco Unity Connection 10.x

# Deleting a Custom Recording in Cisco Unity Connection 10.x

### To Delete a Custom Recording

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Custom Recordings**.

**Step 2** On the **Search Custom Recordings** page, select the check box adjacent to the display name of the custom recording that you want to delete.

**Note** If the custom recording that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

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

**Step 4** In the dialog box that asks you to confirm the deletion, select **OK**.

**Note**

- If you have deleted the recording, which is selected in the **Play After Message Recording** option, then on the **Edit Message Settings** page, the **Recording Selection** option will be disabled and the **System Default Recording** option will be selected.
- If you have deleted the recording, which is selected in the **Post Greeting Recording** option, then on the **Edit Post Greeting Recording Settings** page, the **Recording Selection** will be changed to **None** and the **Do Not Play Recording** option will be selected.

# Managing Call Routing Tables in Cisco Unity Connection 10.x

See the following sections:


- Overview of Default Call Routing Rules in Cisco Unity Connection 10.x, page 10-1
- Adding Call Routing Rules in Cisco Unity Connection 10.x, page 10-2
- Modifying Call Routing Rules in Cisco Unity Connection 10.x, page 10-2
- Changing Phone Language Settings in Cisco Unity Connection 10.x, page 10-3
- Changing the Order of Call Routing Rules in Cisco Unity Connection 10.x, page 10-3
- Deleting Call Routing Rules in Cisco Unity Connection 10.x, page 10-4


## Overview of Default Call Routing Rules in Cisco Unity Connection 10.x

Cisco Unity Connection has two call routing tables—one for direct calls and one for forwarded calls—that handle calls from users and from unidentified callers.

Direct rules handle calls from users and unidentified callers that are dialed directly to Unity Connection. The predefined direct routing rules are:

- **Attempt Sign-In**—Calls from users are routed to the user sign-in conversation.

**Note** With Cisco Unity Connection 10.0(1) and later, a user can play and record both video and audio greetings, when login via **Attempt Sign-in**.

- **Opening Greeting**—Calls from unidentified callers are routed to the Opening Greeting.

Forwarded rules handle calls that are forwarded to Unity Connection from either a user extension or from an extension that is not associated with a user account (such as a conference room). The predefined forwarded routing rules are:

- **Attempt Forward**—All calls forwarded from a user extension are routed to the user greeting.

**Note** With Cisco Unity Connection 10.0(1) and later, a user can play both video and audio greetings, when the calling user receives unanswered call.

- **Opening Greeting**—Calls forwarded from an extension that is not associated with a user account are routed to the Opening Greeting.

You can change the order of the **Attempt Sign-In** and **Attempt Forward** rules relative to additional rules that you add in the respective routing tables, but the Opening Greeting rule is always the last entry for both tables. You cannot delete the predefined rules.

When you create a new rule, you need to specify only the criteria that are used to route the call, and can leave the other fields on the page blank. A blank field matches everything. For example, if you leave the Ports field blank, the rule applies to calls from all ports.

# Adding Call Routing Rules in Cisco Unity Connection 10.x

### To Add a Call Routing Rule

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, select **Direct Routing Rules**. For forwarded calls, select **Forwarded Routing Rules**.

**Step 2** On the **Direct Routing Rules** or **Forwarded Routing Rules** page, select **Add New**.

**Step 3** On the **New Direct Rule** or **New Forwarded Rule** page, enter the name of the new rule in the Display Name field.

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

**Step 5** On the **Edit Direct Rule** or **Edit Forwarded Rule** page, continue entering applicable settings. (For field information, on the **Help** menu, select **This Page**.)

**Note** When you create a new rule, you need to specify only the criteria that are used to route the call, and can leave the other fields on the page blank. A blank field matches everything. For example, if you leave the **Ports** field blank, the rule applies to calls from all ports.

**Step 6** When you have finished entering settings, select **Save**.

# Modifying Call Routing Rules in Cisco Unity Connection 10.x

### To Modify a Call Routing Rule

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, select **Direct Routing Rules**. For forwarded calls, select **Forwarded Routing Rules**.

**Step 2** On the **Direct Routing Rules** or **Forwarded Routing Rules** page, select the display name of the call routing rule that you want to modify.

**Step 3** On the **Edit Direct Routing Rule** or **Edit Forwarded Routing Rule** page, change settings as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Note** A blank field matches everything. For example, if you leave the **Ports** field blank, the rule applies to calls from all ports.

**Step 4** When you have finished entering settings on the page, select **Save**.

**Note** **Default Call Routing Rule** when set to be inactive can cause a call to loop.Verify all calls are routed correctly while modifying **Routing Rule**.

# Changing Phone Language Settings in Cisco Unity Connection 10.x

### To Change Phone Language Settings for a Routing Rule

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, select **Direct Routing Rules**. For forwarded calls, select **Forwarded Routing Rules**.

**Step 2** On the **Direct Routing Rules** or **Forwarded Routing Rules** page, select the display name of the call routing rule that you want to modify.

**Step 3** On the **Edit Direct Routing Rule** or **Edit Forwarded Routing Rule** page, select **Use System Default Language** or **Inherit Language from Caller**, or select one of the languages in the list.

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

# Changing the Order of Call Routing Rules in Cisco Unity Connection 10.x

### To Change the Order of Call Routing Rules

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, select **Direct Routing Rules**. For forwarded calls, select **Forwarded Routing Rules**.

**Step 2** On the **Direct Routing Rules** or **Forwarded Routing Rules** page, select **Change Order**.

**Step 3** On the **Edit Direct Routing Rule Order** or **Edit Forwarded Routing Rule Order** page, in the **Reorganization** list, select the name of a rule that you want to move, then select the down or up arrow as applicable.

**Step 4** When you have finished reordering the rules, select **Save**.

# Deleting Call Routing Rules in Cisco Unity Connection 10.x

### To Delete a Call Routing Rule

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then expand **Call Routing**. For direct calls, select **Direct Routing Rules**. For forwarded calls, select **Forwarded Routing Rules**.

**Step 2** On the **Direct Routing Rules** or **Forwarded Routing Rules** page, check the check box adjacent to the display name of the rule that you want to delete.

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

**Step 4** In the dialog box that asks you to confirm the deletion, select **OK**.

# Managing Video Greetings in Cisco Unity Connection 10.x

See the following sections:


- Overview of Video Greetings in Cisco Unity Connection, page 11-1
- Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x, page 11-5
- Installing, Integrating, and Accessing Cisco MediaSense, page 11-3
- Pre-checks Required for Video Greetings, page 11-9


## Overview of Video Greetings in Cisco Unity Connection

Cisco Unity Connection 10.0(1) is a feature-rich voice messaging platform that now provides immersive experience of video greetings. Video greetings add personal touch to the user greetings. Unity Connection facilitates the user to record and play video greetings for the identified callers using a video endpoint. For the outside callers, Unity Connection only plays the video greetings depending on the class of service configuration.

**Note**

- Outside callers are those who are not Unity Connection users, however, calling from a supported video endpoint—the caller can call the user extension and be forwarded to Unity Connection when the user does not answer, and then the call be will video only depending on the class of service configuration.
- A video endpoint is a telephone with a video display, which allows users to record and play video greetings.

To enable the video greetings feature for a user, the administrator needs to create video services accounts for a user and configure it with the video services. Video services allow Unity Connection to integrate with video server for the storage and retrieval of video greetings recorded by the user. For more information on video services and video service accounts, see Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x, page 11-5.Unity Connection

**Note** For video servers, Unity Connection 10.0(1) only integrates with Cisco MediaSense video server.

Cisco MediaSense supports recording, playback, and storage of media, including audio and video recording. Unity Connection does not integrate with Cisco MediaSense cluster for the storage and retrieval of video greetings. Only single Cisco MediaSense node is supported with Unity Connection. With Unity Connection 10.0(1) only the standard Cisco MediaSense video server is integrated, which is installed using one of the Cisco-provided OVA templates. If an incorrect OVA template is used, or if the virtual machine's configuration is changed after the OVA template is applied, the server is considered to be not supported.For more information on integrating Cisco MediaSense with Unity Connection, see Installing, Integrating, and Accessing Cisco MediaSense, page 11-3.

**Note** If the state of video server is unavailable or the resources get exhausted:

- When establishing a video call, Unity Connection will not treat the call as video.
- When recording or playing video greetings, Unity Connection will downgrade the call to audio.

We recommend that you enable the video greetings feature in IPv4 mode only. Video greetings are not supported in both the IPv6 and dual (IPv4/IPv6) modes.

When a call comes, Unity Connection applies all the pre-checks required to establish a video call. A user will be able to record and play video greetings, if all the pre-checks required for each video call are satisfied. For more information on pre-checks, see Pre-checks Required for Video Greetings, page 11-9.

After configuring video greetings a user will be able to successfully record and play video greetings. Cisco Unity Connection 10.0(1) has enhanced the current greeting experience by providing the video greetings to the caller. Unity Connection users login via direct sign-in using the telephone user interface (touchtone conversation) to record and play video greetings, which is supported by the setup options and self-enrollment. A user can play video greetings, when the calling user receives unanswered call (“ring-no-answer”) from the called user. For more information on recording video greetings using telephone user interface, see the “Enabling Users to Play and Record Video Greetings” section of the “Managing Your Personal Greetings” chapter in the *User Guide for the Cisco Unity Connection Phone Interface*.

**Note** In case of a video call, voice-recognition conversation is not supported. For more information on voice recognition conversation, see the Touchtone and Voice-Recognition Conversations, page 16 section of the Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x chapter.

For more information on direct sign-in and ring-no-answer using attempt forward, see the “Enabling a User Greeting” section on page 4-62 of the Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x chapter.

To allow the playback of video greetings for each user, enable the My Personal Recording option in the Callers See section. For more information on Callers See and Callers Hear settings, see the Allowing Users to Playback Video Greetings in Cisco Unity Connection 10.x, page 16-14 section in the Changing Conversation Settings for All Users in Cisco Unity Connection 10.x, page 16-1 chapter of *System Administration Guide for Cisco Unity Connection* and the “Edit Greeting” Section of the Cisco Unity Connection 10.x Template Settings chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

# Installing, Integrating, and Accessing Cisco MediaSense

Cisco MediaSense is a video server that integrates with Unity Connection to support the recording, playback, and storage of audio and video recordings. Cisco MediaSense has a default setting of pruning enabled for 60 days, which means that MediaSense deletes all video greetings after 60 days and will not be available any more. To avoid your video greetings getting deleted, disable the MediaSense Prune Policy setting.

This section explains the procedures:

- Installing and Integrating Cisco MediaSense
- Accessing Cisco MediaSense AdministrationTo access Cisco MediaSense Administration
- Uploading Cisco logo from Cisco MediaSense
- Supported Specifications of a Customized logo
- Disabling Cisco MediaSense Prune Policy

## Installing and Integrating Cisco MediaSense

**To install and integrate Cisco MediaSense with Unity Connection 10.0(1)**

**Step 1** To download and install Cisco MediaSense, see the "Cisco MediaSense Installation" chapter at

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/mediasense/901/inst_admin/CUMS_BK_IFE33F4B_00_mediasense-install-and-admin-guide_chapter_010.html

**Step 2** When the Cisco MediaSense is installed successfully, integrate the Cisco MediaSense with Unity Connection.

**Step 3** To integrate, enter the Cisco MediaSense IP address or hostname in the Video Server field while creating or modifying video services. For More information on creating and modifying video services, see the Modifying Video Service in Cisco Unity Connection 10.x, page 11-6.

**Note** The Video Server(1) field only support IPv4 address and hostname.

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

## Accessing Cisco MediaSense Administration

**To access Cisco MediaSense Administration**

**Step 1** From a web browser on any computer in your Unified Communications network, go to *http://servername/oraadmin*.

The servername is the IP address of the server where you have installed Cisco MediaSense.

**Step 2** A **Security Alert** message may appear, prompting you to accept the self-signed security certificate, if you have not already installed it. This certificate is required for a secure connection to the server. Click the required button. This security message may not appear if you have already installed a security certificate. The **Cisco MediaSense Administration Authentication** page appears.

**Step 3** Enter the **Application Administrator User ID** and **password** for the server. Click **Log In**.

# Uploading Cisco logo from Cisco MediaSense

**To upload Cisco logo from Cisco MediaSense**

**Step 1** From the **Cisco MediaSense Administration** menu, select **Media File Management**.

**Step 2** On the **Media File Management** toolbar, click **Add**.

**Step 3** On the **Add Media File** screen, enter a title for the image to be uploaded. Make sure that the title name of the image should be **CiscoUnityConnectionLogo.mp4**.

**Step 4** (*Optional*) Enter a description of the file.

**Step 5** Browse and select the Cisco logo in the **File** field.

**Note** You can either select a customized logo from your system or can select the standard Cisco logo.

**Step 6** Click **Save**.

# Supported Specifications of a Customized logo

The customized logo must be added must be in MP4 format and meet the following specifications:

- H.264 constrained baseline profile
- Resolution 1080p, 720p, 480p, or 360p
- Audio AAC-LC (MediaSense converts it to AAC-LD upon import)
- 48000 Hz sampling frequency
- Mono
- Maximum 2GB file size

# Disabling Cisco MediaSense Prune Policy

**To disable Cisco MediaSense Prune Policy**

**Step 1** From the Cisco MediaSense Administration menu, select **Prune Policy Configuration**.

**Step 2** On the **MediaSense Prune Policy Configuration** page, uncheck the **Automatically prune recordings after they are more than 60 days old, and when disk space is needed for new recordings (1)** checkbox.

**Step 3** Click **Save**.

**Step 4** Restart all the **Cisco MediaSense** media services on all the nodes.

# Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x

In Cisco Unity Connection version 10.0(1), a new feature of video greetings is introduced. To enable the video greetings feature, the administrator needs to create the video services. The video services are then configured with each user using the video service account. Video services allow Unity Connection to integrate with video server to store and retrieve all the video greetings recorded by the user. In addition, it allows Unity Connection to verify the state of video server, codecs, and user credentials used with video server.

See the following sections:


- Creating Video Service in Cisco Unity Connection 10.x, page 11-5
- Modifying Video Service in Cisco Unity Connection 10.x, page 11-6
- Creating Video Services Accounts in Cisco Unity Connection 10.x, page 11-7
- Deleting Video Service Account in Cisco Unity Connection 10.x, page 11-8
- Using the Cisco Unity Connection 10.x Bulk Administration Tool to Manage Video Services Accounts, page 11-8


## Creating Video Service in Cisco Unity Connection 10.x

### To Create a New Video Service

**Step 1** In Cisco Unity Connection Administration, navigate to **Video > Video Services**.

**Step 2** On the **Search Video Service** page, select **Add New**.

**Step 3** On the **New Video Service** page, select the type of video service from the drop down box and enter a display name. **Default value: MediaSense**.

**Note** Fields marked with * (an asterisk) are required.

**Step 4** Select **Save or Test**.

**Note** The administrator can see the **Tasks Execution Results**, when selects the **Status** image on the **Search Video Service** page and the **Test** button on the **New Video Service** page.

Note the following:

- When the **Test** button is selected, Unity Connection displays the **Tasks Execution Results**:
  - **Video server state:** Displays whether Unity Connection is able to ping the IP address, FQDN, or hostname of video server.
  - **Video server certificates:** Displays the failure while validating video server certificates.
  - **Credentials verification:** Displays the authentication results of user credentials on video server.
  - **Media capabilities:** Displays the list of codecs used with video server.

For more information on the error messages, see the Troubleshooting Video Greetings in Cisco Unity Connection 10.0(1) chapter in the *Troubleshooting Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx.html.

For More information on status image, see the "Search Video Services" section on page 10-1 of the Video Settings in Cisco Unity Connection 10.x chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

# Modifying Video Service in Cisco Unity Connection 10.x

### To Modify a Video Service

**Step 1** In Cisco Unity Connection Administration, navigate to **Video > Video Services**.

**Step 2** On the **Search Video Service** page, select the display name of the video service that you want to modify.

**Step 3** On the **Edit Video Service** page, change settings as applicable. (For field information, on the fields on the **Edit Video Service** page, navigate to **Help > This Page**.)

**Step 4** When you have finished changing settings on the **Edit Video Service** page, select **Save or Test**.

**Note** The administrator can see the **Tasks Execution Results**, when selects the **Status** image on the **Search Video Service** page and the Test button on the **New Video Service** page.

Note the following:

- When the **Test** button is selected, Unity Connection displays the **Tasks Execution Results**:
  - **Video server state:** Displays whether Unity Connection is able to ping the IP address, FQDN, or hostname of video server.
  - **Video server certificates:** Displays the failure while validating video server certificates.
  - **Credentials verification:** Displays the authentication results of user credentials on video server.
  - **Media capabilities:** Displays the list of codecs used with video server.

For more information on the error messages, see the Troubleshooting Video Greetings in Cisco Unity Connection 10.0(1) chapter in the *Troubleshooting Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx.html.

For More information on status image, see the "Search Video Services" section on page 10-1 of the Video Settings in Cisco Unity Connection 10.x chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

# Creating Video Services Accounts in Cisco Unity Connection 10.x

See the following sections:


- To Add a Video Service Account for an Individual User or User Template to Access Video Service, page 11-7
- To Map Video Services Accounts for Multiple User Accounts in Bulk Edit Mode, page 11-8


### To Add a Video Service Account for an Individual User or User Template to Access Video Service

**Step 1** In Cisco Unity Connection Administration, find the user account or user template that you want to edit.

**Step 2** On the **Edit** menu, select **Video Services Accounts**.

**Step 3** On the **Video Services Accounts** page, select **Add New**.

**Note** For each user, you can add only one video service account.

**Step 4** On the **New Video Services Accounts** page, in the **Video Service** list, select the display name of the service that you want to configure with the video service account.

**Step 5** *(Display Only)* In the **Service Type** field, the type of server to which the video service account connects is added by default.

**Step 6** Select the **Map Video Service** check box to configure the video service with video service account.

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

**Note** If there are no video services, Unity Connection displays an error message and asks you to create a video service on the **Video Services Accounts** page.

When selected the **Save** button, a status icon appears on the **Video Services Accounts** page. The status icon that indicates the status of the video service account for a Cisco Unity Connection user:

- **Success image:** Displays **No problems found** when the video service is added. When the administrator selects this image, Cisco Unity Connection displays the successful status on the **Task Execution Results** page.
- **Warning image:** Displays **One or more problems found** when the video service is added. When the administrator selects this image, Cisco Unity Connection displays the error status on the **Task Execution Results** page.

The **Task Execution Results** page displays the following information:

- **Video service enabled:** Displays whether the user has enabled the video service or not.
- **Video server state:** Displays whether Unity Connection is able to ping the IP address, FQDN, or hostname of the video server.
- **Credentials verification:** Displays the authentication results of user credentials on video server.

- **Media capabilities:** Displays the list of codecs used with the video server.
- **Video capabilities:** Displays whether the video settings in the **Edit Class of Service** page are enabled or not.

#### To Map Video Services Accounts for Multiple User Accounts in Bulk Edit Mode

**Step 1** In Cisco Unity Connection Administration, on the **Search Users** page, select the applicable user check boxes, and select **Bulk Edit**.

If the user accounts that you want to edit in bulk do not all appear on one **Search** page, select all applicable check boxes, and then select **Bulk Edit**.

**Step 2** On the **Edit** menu, select **Video Services Accounts**.

**Note** If there are no video services, Unity Connection displays an error message and asks you to create a video service on the **Bulk Edit Video Service Accounts** page.

**Step 3** On the **Video Services Accounts** page, select the **Map Video Service** check box to associate video service accounts of the users with their respective video services.

**Step 4** Select **Submit**.

# Deleting Video Service Account in Cisco Unity Connection 10.x

#### To Delete a Video Service Account for an Individual User

**Step 1** In Cisco Unity Connection Administration, find the user account that you want to edit.

**Step 2** On the **Edit** menu, select **Video Service Accounts**.

**Step 3** On the **Video Service Accounts** page, select the check box adjacent to the display name of the video service account that you want to delete.

**Step 4** Select **Delete Selected**.

**Step 5** In the dialog box that asks you to confirm the deletion, select **OK**.

# Using the Cisco Unity Connection 10.x Bulk Administration Tool to Manage Video Services Accounts

The Bulk Administration Tool allows you to create, update, and delete multiple video services accounts at the same time by importing information contained in a comma separated value (CSV) file. In addition, it allows you to export information about video service accounts from Cisco Unity Connection to a CSV file.

**To Access the Bulk Administration Tool**

**Step 1** In Cisco Unity Connection Administration, navigate to Tools.

**Step 2** Select **Bulk Administration Tool**.

To learn more about using the tool, see the "Using the Cisco Unity Connection 10.x Bulk Administration Tool" appendix.

# Pre-checks Required for Video Greetings

Pre-checks are required to establish a video call. A user will be able to record and play video greetings, if the pre-checks for each video call are satisfied.

**Note** Unity Connection will make the call as audio:

- If any one of the pre-checks required to establish a video call is not met.
- If the primary DNS is unresponsive and the response time is more than one second.

When the calling user receives unanswered call (“ring-no-answer”) from the called user, the calling user receives video greetings of the calling user. Cisco Unity Connection performs the following pre-checks before treating a call as video and allowing the calling user to play video greetings:

1. **Identification of Caller Type:** Cisco Unity Connection supports two types of callers; identified callers and unidentified callers. Unity Connection verifies whether the calling user is an identified or unidentified caller. To play video greetings to the unidentified callers, Unity Connection verifies whether the administrator has enabled the **Outside Callers** option in the class of service (COS) settings.
2. **Identification of Video EndPoint:** Cisco Unified Communications Manager (CUCM) identifies whether the calling user is using a video phone or an audio phone to play greetings.
3. **Enabling Class of Service (COS) settings:** The class of service (COS) allow users with mailboxes to enable video greetings feature. Unity Connection verifies whether the administrator has enabled the video greeting settings in the class of service for both the calling user and called user. For more information on Class of Service Settings (COS), see the “Cisco Unity Connection 10.x Class of Service Settings” section of “Cisco Unity Connection 10.x Class of Service Settings” chapter in the Interface Reference Guide for Cisco Unity Connection Administration at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui/guide/10xcucguix.html.
4. **Mapping users to Video Services Accounts:** To access the video greetings feature, a user needs a video service configure with the video service account. Unity Connection verifies the mapping of video services accounts for both the calling user and called user. For more information on video services accounts, see the Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x, page 11-5.

**Note** For each user, you can add one video service account.

5. **Identification of video server state:** Unity Connection integrates with video server for the storage and retrieval of video greetings and verifies whether the video server state active or not. For more information on video server state, see the Modifying Video Service in Cisco Unity Connection 10.x, page 11-6.
6. **Verification of the Concurrent sessions limit:** Unity Connection supports only 25 video sessions and session limits at a time and verifies whether the current video call is not exceeding the concurrent session limits. For more information on concurrent session limits, see the Video Settings in Cisco Unity Connection 10.x chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

When a user record and play video greetings to single or multiple users, Cisco Unity Connection verifies the following pre-checks before allowing the user to record and play a video greeting:

1. **Identification of Video EndPoint:** A video endpoint is a telephone with a video display, which allows users to record and play video greetings. Cisco Unified Communications Manager (CUCM) identifies whether the calling user is using a video phone or an audio phone to play greetings.
2. **Mapping users to Video Services Accounts:** To access the video greetings feature, a user needs a video service configure with the video service account. Unity Connection verifies the mapping of video services accounts for both the calling user and called user. For more information on video services accounts, see the Configuring Video Services and Video Services Accounts in Cisco Unity Connection 10.x, page 11-5.

**Note** For each user, you can add one video service account.

3. **Enabling Class of Service (COS) settings:** The class of service (COS) allow users with mailboxes to enable video greetings feature. Unity Connection verifies whether the administrator has enabled the video greeting settings in the class of service for both the calling user and called user. For more information on Class of Service Settings (COS), see the “Cisco Unity Connection 10.x10.x Class of Service Settings” section of “Cisco Unity Connection 10.x Class of Service Settings” chapter in the Interface Reference Guide for Cisco Unity Connection Administration http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui/guide/10xcucguix.html.
4. **Identification of video server state:** Unity Connection integrates with video server for the storage and retrieval of video greetings and verifies whether the video server state active or not. For more information on video server state, see the Modifying Video Service in Cisco Unity Connection 10.x, page 11-6.
5. **Verification of the Concurrent sessions limit:** Unity Connection supports only 25 video sessions and session limits at a time and verifies whether the current video call is not exceeding the concurrent session limits. For more information on concurrent session limits, see the Video Settings in Cisco Unity Connection 10.x chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

# Managing Schedules and Holidays in Cisco Unity Connection 10.x

See the following sections:


- Overview of Default Schedules in Cisco Unity Connection 10.x, page 12-1
- Designating Holidays in Cisco Unity Connection 10.x, page 12-1
- Creating Schedules in Cisco Unity Connection 10.x, page 12-2
- Modifying Schedules in Cisco Unity Connection 10.x, page 12-2
- Deleting Schedules in Cisco Unity Connection 10.x, page 12-3


## Overview of Default Schedules in Cisco Unity Connection 10.x

Cisco Unity Connection has three predefined schedules: All Hours, Weekdays, and Voice Recognition Update Schedule. You can modify but not delete the predefined schedules.

By default, the **All Hours schedule** is configured to be active 24 hours a day, 7 days a week, with no holidays; routing rules that follow this schedule are always active, and call handlers that use this schedule never use closed hour transfer settings or play closed greetings.

The **Weekdays schedule** is configured to be active from 8 a.m. to 5 p.m. (in the time zone of the Unity Connection server) from Monday through Friday. It is also configured to observe any days and times that are set in the default Holidays schedule. Note however that by default the Holidays schedule is not preconfigured for any days or times. At a minimum you may want to update the Holidays schedule to add days and times when your organization is closed.

The **Voice Recognition Update schedule** dictates the times and days when the Unity Connection voice-recognition transport utility can automatically rebuild the voice-recognition name grammars if there are pending changes. By default, all days and times are active for this schedule; however, because of the potential system performance impact associated with rebuilding large name grammars, you may want to edit this schedule to create blackout times and days during periods of heavy system usage.

## Designating Holidays in Cisco Unity Connection 10.x

When a Holiday setting is in effect, Cisco Unity Connection plays holiday greetings (if enabled) and observes closed hours transfer rules. You can set up several years of holidays at a time. Because many holidays occur on different dates each year, confirm that the holiday schedule remains accurate annually.

### To Add a Holiday Schedule

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Holiday Schedules**.

**Step 2** On the **Search Holiday Schedules** page, select **Add New**.

**Step 3** On the **New Holiday Schedule** page, enter a display name for the holiday schedule, and select **Save**.

**Step 4** To add a new holiday to the schedule, on the **Edit Holiday Schedule Basics** page, select **Add New**.

**Step 5** On the **New Holiday** page, enter settings as applicable. (For field information, on the **Help** menu, select **This Page**.)

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

**Step 7** To return to the **Edit Holiday Schedule** page, on the **Edit** menu, select **Holiday Schedule Basics**.

# Creating Schedules in Cisco Unity Connection 10.x

### To Create a New Schedule

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Schedules**.

**Step 2** On the **Search Schedules** page, select **Add New**.

**Step 3** On the **New Schedule** page, enter a display name, and select a holiday schedule to apply to this schedule.

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** To add time frames when the schedule is active, on the **Edit Schedule Basics** page, in the **Schedule Details** box, select **Add New**.

**Step 6** On the **New Schedule Detail** page, enter settings as applicable. (For field information, on the **Help** menu, select **This Page**.)

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

**Step 8** To return to the **Edit Schedule** page, on the **Edit** menu, select **Schedule Basics**.

# Modifying Schedules in Cisco Unity Connection 10.x

### To Modify a Schedule

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Schedules**.

**Step 2** On the **Search Schedules** page, select the display name of the schedule that you want to modify.

**Note** If the schedule that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Schedule Basics** page, change the display name or holiday schedule settings, as applicable.

**Step 4** When you have finished changing settings on the **Edit Schedule** page, select **Save**.

**Step 5** To add time frames when the schedule is active, in the **Schedule Details** box, select **Add New**.

**Step 6** If you change any settings on the **New Schedule Detail** page, select **Save**. To return to the Edit Schedule page, on the **Edit** menu, select **Edit Schedule**.

**Step 7** To remove time frames, check the check box next to the schedule detail that you want to remove, and select **Delete Selected**.

**Note** If you remove all schedule details from a schedule, the schedule is never active. Call handlers and users that use this schedule as-is will always use the closed hours transfer settings, and the closed greeting always plays (if enabled) except when it is overridden by the holiday, internal, busy, or alternate greeting.

# Deleting Schedules in Cisco Unity Connection 10.x

### To Delete a Schedule

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Schedules**.

**Step 2** On the **Search Schedules** page, check the check box adjacent to the display name of the schedule that you want to delete.

**Note** If the schedule that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

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

**Note** If the schedule that you are attempting to delete is referenced by a call routing table or call handler, you receive an error message and are not able to delete the schedule until you find and remove the reference.

**Step 4** In the dialog box that asks you to confirm the deletion, select **OK**.

# Managing Restriction Tables in Cisco Unity Connection 10.x

See the following sections:


- Overview of Default Restriction Tables in Cisco Unity Connection 10.x, page 13-1
- Creating Restriction Tables in Cisco Unity Connection 10.x, page 13-2
- Modifying Restriction Tables in Cisco Unity Connection 10.x, page 13-3
- Deleting Restriction Tables in Cisco Unity Connection 10.x, page 13-3


## Overview of Default Restriction Tables in Cisco Unity Connection 10.x

Cisco Unity Connection comes with the following predefined restriction tables, which you can modify (including changing their names) but not delete. By default, each of these restriction tables prevents access to long distance phone numbers.

| | |
|---|---|
| **Default Fax** | Restricts numbers for fax delivery. |
| **Default Outdial** | Restricts numbers for message notifications. Also restricts the user extensions that Unity Connection dials when the phone is selected as the recording and playback device in the Media Master. |
| **Default System Transfer** | Restricts numbers that can be used for Caller system transfers, which allow unidentified callers to transfer to a number that they specify. For example, callers may want to dial a lobby or conference room phone that is not associated with a Unity Connection user. By default, the table does not allow Unity Connection to dial any numbers. |
| **Default Transfer** | Restricts numbers for call transfers. |
| **User-Defined and Automatically-Added Alternate Extensions** | Restricts the numbers the users can use to create alternate extensions for themselves through interfaces such as the Cisco Personal Communications Assistant or via an API call. Also restricts numbers from being offered as alternate extensions. For example, you might block a lobby or conference room extension so that users who frequently call Unity Connection from those shared phones are not automatically prompted to add the number as an alternate extension. |

| | |
|---|---|
| **Excluded Extensions for Automatically Added Alternate Extensions** | Restricts numbers from being offered as alternate extensions. For example, you might add a lobby or conference room extension so that users who frequently call Unity Connection from those shared phones are not automatically prompted to add the number as an alternate extension. |

See the "How Restriction Tables Work" section on page 4-7 for a detailed discussion of how restriction tables function.

# Creating Restriction Tables in Cisco Unity Connection 10.x

You can modify the predefined restriction tables, and you can create up to 100 new ones. You can also add up to 100 dial strings to a table. New dial strings are automatically inserted into the restriction table as Dial String 0. Note that the order of the dial strings is very important because Cisco Unity Connection sequentially compares a phone number to the call patterns in the restriction table, starting with Dial String 0. If a number matches more than one call pattern, the number is handled according to the first call pattern it matches.

You can indicate call patterns by entering specific numbers or by using the following special characters as wildcards:

| | |
|---|---|
| * | Matches zero or more digits. |
| ? | Matches exactly one digit. Use? as a placeholder for a single digit. |
| # | Corresponds to the # key on the phone. |

By default, all restriction tables have * as the call pattern in the last dial string of the table. You cannot modify this call pattern setting, as it prevents a case in which the entered number does not match any call pattern in the table. However, you can change the Blocked field setting for this dial string to either permit or restrict a number.

### To Create a New Restriction Table

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Restriction Tables**.

**Step 2** On the **Search Restriction Tables** page, select **Add New**.

**Step 3** On the **New Restriction Table** page, enter basic settings as applicable. (For field information, on the Help menu, select **This Page**.)

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** To add patterns to the restriction table, on the **Edit Restriction Table Basics** page, in the **Restriction Patterns** box, select **Add New**.

**Step 6** If you change any settings on the pattern, select **Save**.

**Step 7** Repeat Step 5 and Step 6 until you have added each pattern that you want to allow or restrict.

**Step 8** To change the order of the patterns, select **Change Order**, and then do the following sub-steps:

a. To move a pattern within the list, on the **Change Restriction Pattern Order** page, select the pattern, then select the down or up arrows as applicable.

b. When you have finished reordering the patterns, select **Save**.

c. To return to the **Edit Restriction Table** page, on the **Edit** menu, select **Restriction Table Basics**.

**Step 9** To delete a pattern in the list, check the check box to the left of the pattern, select **Delete Selected**, then select **OK** to confirm the deletion.

# Modifying Restriction Tables in Cisco Unity Connection 10.x

### To Modify a Restriction Table

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Restriction Tables**.

**Step 2** On the **Search Restriction Tables** page, select the display name of the restriction table that you want to modify.

**Note** If the restriction table that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** To add patterns to the restriction table, on the **Edit Restriction Table Basics** page, in the **Restriction Patterns** box, select **Add New**.

**Step 4** If you change any settings on the pattern, select **Save**.

**Step 5** Repeat Step 3 and Step 4 until you have added each pattern that you want to allow or restrict.

**Step 6** To delete a pattern in the list, check the check box to the left of the pattern, and select **Delete Selected**, then select **OK** to confirm the deletion.

**Step 7** To change the order of the patterns, select **Change Order**, and then do the following sub-steps:

a. To move a pattern within the list, on the **Change Restriction Pattern Order** page, select the pattern, then select the down or up arrows as applicable.

b. When you have finished reordering the patterns, select **Save**.

c. To return to the **Edit Restriction Table** page, on the **Edit** menu, select **Restriction Table Basics**.

# Deleting Restriction Tables in Cisco Unity Connection 10.x

### To Delete a Restriction Table

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Restriction Tables**.

**Step 2** On the **Search Restriction Tables** page, check the check box adjacent to the display name of the restriction table that you want to delete.

**Note** If the restriction table that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

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

**Note** If the restriction table you are attempting to delete is referenced by a class of service, you receive an error message and are not able to delete the table until you find and remove the reference.

**Step 4** In the dialog box that asks you to confirm the deletion, select **OK**.

# Setting Up System Transfers in Cisco Unity Connection 10.x

See the following sections:


- System Transfer Overview in Cisco Unity Connection 10.x, page 14-1
- Task List: Offering Caller System Transfers in Cisco Unity Connection 10.x, page 14-2
- Task List: Offering User System Transfers in Cisco Unity Connection 10.x, page 14-4


## System Transfer Overview in Cisco Unity Connection 10.x

In your organization, you may find that callers want to be able to dial numbers that are not typically listed in the corporate directory. For example, users and outside callers may find it convenient to be able to call Cisco Unity Connection and transfer from the Opening Greeting or another call handler to a lobby extension, conference room extension, or an extension assigned to someone in the organization who is not a Unity Connection user, such as an employee who is visiting from another site and is using a guest office. In addition, some users may want to be able to call Unity Connection and then transfer to phone numbers outside of the organization—such as frequently called customers or vendors—so that they do not have to hang up after checking messages to place another call, or so that they do not incur long-distance charges while on business travel.

You can configure individual user or call handler greetings to allow callers to transfer to numbers that are not associated with Unity Connection users or call handlers. Alternatively, you can route callers to one of two "system transfer" conversations, both of which offer callers the ability to transfer to numbers that are not associated with Unity Connection users:

| | |
|---|---|
| **Caller System Transfer** | This conversation prompts callers to enter the number that they want to transfer to.<br><br>To help protect your organization from toll fraud and unauthorized use, Unity Connection performs the transfer only when the Default System Transfer restriction table permits it. |
| **User System Transfer** | This conversation prompts callers to sign in to Unity Connection. After callers enter their Unity Connection IDs and PINs, Unity Connection prompts them to enter the number that they want to transfer to.<br><br>To help protect your organization from toll fraud and unauthorized use, Unity Connection performs the transfer only when permitted by the transfer restriction table that is associated with the class of service for the user who signed in. |

You can route callers to either system transfer conversation in several ways, including:

- By creating a new phone number (on your phone system) and a corresponding routing rule to send callers to either system transfer conversation. When callers dial the number, Unity Connection sends calls to the system transfer conversation that you specify.
- By offering a system transfer as a "one-key dialing" option. You can specify either system transfer (on the Caller Input page for any call handler or user greeting) as the action that Unity Connection performs when a caller presses a particular key during the greeting.

  For example, to allow all callers to transfer to a lobby phone, guest office, or a conference room from the Opening Greeting, you could set Unity Connection to offer Caller System Transfers when callers press 3. To offer system transfers to a particular user, you could set Unity Connection to offer User System Transfers when the user presses a particular key during the Opening Greeting or even while listening to his or her own greeting.

Regardless of how you offer callers either type of system transfer, as long as the number entered by the caller is allowed by the Default System Transfer restriction table, Unity Connection releases calls to the phone system, which handles the transfer to the specified number. This means that users and outside callers cannot return to the Unity Connection phone menus after the transfer takes place.

Follow the instructions in the applicable task list to set up Caller and User System Transfers:

- Task List: Offering Caller System Transfers in Cisco Unity Connection 10.x, page 14-2
- Task List: Offering User System Transfers in Cisco Unity Connection 10.x, page 14-4

When using either the Caller System Transfer or User System Transfer conversation, Unity Connection prompts users and callers to confirm the number that they enter before performing the transfer. To disable the confirmation prompt, change the **System Transfers: Confirm Number Before Transfer** setting on the **System Settings > Advanced > Conversations** page in Cisco Unity Connection Administration. For details, see the "Conversation Configuration" section in the "Cisco Unity Connection 10.x Advanced Settings" chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

# Task List: Offering Caller System Transfers in Cisco Unity Connection 10.x

1. Modify the Default System Transfer restriction table so that callers can dial numbers that you want to allow. See the "Managing Restriction Tables in Cisco Unity Connection 10.x" chapter for details on how restriction tables work and how to modify them.
2. Configure one of the following methods for callers to access system transfers:
   - **Configure a greeting**—Each user and call handler greeting can be enabled to allow system transfers. See the "Configuring a Greeting to Allow System Transfers" section on page 14-3.
   - **Set up a one-key dialing option**—Use caller input settings for a call handler to send callers to the Caller System Transfer conversation when they press the key that you specify during a call handler greeting. Then, enable caller input for the applicable greeting and rerecord the greeting to mention the key that callers can press in the call handler greeting (for example, "...to reach a conference room, press 3.").

– **Set up a "system transfers" phone number**—See the documentation for the phone system to set up a new phone number. Then, on the **Call Management > Call Routing > Direct Routing Rules** page in Cisco Unity Connection Administration, create a routing rule that sends any call that arrives for the new number to the Caller System Transfer conversation. Distribute the new number to callers who will find Caller System Transfers convenient.

# Configuring a Greeting to Allow System Transfers

The easiest way to offer system transfers in your organization is to configure user and call handler greetings to allow system transfers. Do one of the following procedures:

- To Configure an Individual Greeting to Allow System Transfers, page 14-3
- To Configure Multiple Greetings to Allow System Transfers in Bulk Edit Mode, page 14-3

### To Configure an Individual Greeting to Allow System Transfers

**Step 1** In Cisco Unity Connection Administration, go to the **Greetings** page for the applicable user, user template, call handler, or call handler template.

**Step 2** Select the applicable greeting.

**Step 3** On the **Edit Greeting** page, check the **Allow Transfers to Numbers Not Associated with Users or Call Handlers** check box.

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

### To Configure Multiple Greetings to Allow System Transfers in Bulk Edit Mode

**Step 1** On the **Search Call Handlers** or **Search Users** page, check the applicable call handler or user check boxes, and select **Bulk Edit**.

If the call handlers or users that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable call handlers or users. Then select **Bulk Edit**.

**Note** The **Status** message at the top of the page tells you how many call handlers or users are being edited. Also note that each page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 2** On the **Edit** menu, select **Greetings**.

**Step 3** On the **Greetings** page, select the display name of the greeting that you want to modify.

**Step 4** On the **Edit Greeting** page, check the left-most check box to select the **Allow Transfers to Numbers Not Associated with Users or Call Handlers** field, and then check the check box.

**Step 5** If applicable, set the **Bulk Edit Task Scheduling** Fields to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 6** Select **Submit**.

# Task List: Offering User System Transfers in Cisco Unity Connection 10.x

1. For the users who will use User System Transfers, modify the transfer restriction table that is associated with the user class of service so that the users can dial numbers that are not associated with Unity Connection entities. See the "Managing Restriction Tables in Cisco Unity Connection 10.x" chapter for details on how transfer restriction tables work and how to modify them to allow the numbers you want.

**Tip** If you are not offering system transfers to all users in a single class of service, reassign applicable users to a new class of service that has a transfer restriction table that allows them to dial the applicable numbers.

2. Configure one of the following methods for callers to access system transfers:
   - **Configure a Custom Keypad Mapping conversation**—Use the Custom Keypad Mapping tool to map a key to the User System Transfer Conversation so that it is offered to users from the main menu. See the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter for details.
   - **Set up a one-key dialing option**—Use caller input settings for a call handler or a user greeting to send callers to the User System Transfer conversation when they press the key that you specify during the greeting. Then, enable caller input for the applicable greeting. Tell users which key to press to access the User System Transfer conversation when they listen to the greeting, or if you are not concerned about other callers hearing the option and not being able to use it, rerecord the greeting to mention the key. (For example, "...to reach a conference room, press 3.")
   - **Set up a "system transfers" phone number**—See the documentation for the phone system to set up a new phone number. Then, on the **Call Management > Call Routing > Direct Routing Rules** page in Cisco Unity Connection Administration, create a routing rule that sends any calls for the new number to the User System Transfer conversation. Distribute the new number only to the users who will use User System Transfers.

# Cisco Unity Connection 10.x Conversation

A Cisco Unity Connection conversation is a set of prerecorded prompts and menu options that callers hear as they interact with Unity Connection by phone. It is organized into two main conversations—one for outside callers and one for Unity Connection users. This chapter summarizes the Unity Connection conversation and the ways that you can customize it.

See the following sections:


- How Outside Callers Interact With Cisco Unity Connection 10.x by Phone, page 15-1
- How Users Interact With Cisco Unity Connection 10.x by Phone, page 15-1
- How Administrators Can Customize the User Conversation in Cisco Unity Connection 10.x, page 15-2
- How Users Can Customize the User Conversation in Cisco Unity Connection 10.x, page 15-5


## How Outside Callers Interact With Cisco Unity Connection 10.x by Phone

When outside callers access Cisco Unity Connection by phone, they hear a set of prerecorded instructions and options known as the outside caller conversation. The outside caller conversation enables callers to access the Unity Connection automated attendant, conduct user searches by using the corporate directory, use call routing options, and play audiotext messages.

## How Users Interact With Cisco Unity Connection 10.x by Phone

When users sign in to Cisco Unity Connection by phone, they hear the user conversation. Its collection of prompts enables users to sign in to Unity Connection, enroll as new Unity Connection users, send and receive messages, record greetings, and change their personal settings.

There are two ways in which users can interact with Unity Connection by phone:

- **Phone keypad keys**—Users press keys on any touchtone phone to respond to prompts, or select menu options.
- **Voice commands**—Users speak into the phone handset, headset, or speakerphone, and Unity Connection responds to their voice commands. Users have the option to press keys on the phone keypad for a primary set of commands rather than say a voice command.

You specify whether users are prompted to use phone keypad keys or voice commands when they sign in to Unity Connection.

# How Administrators Can Customize the User Conversation in Cisco Unity Connection 10.x

There are a number of ways administrators can customize the conversations that callers and users hear as they interact with Cisco Unity Connection.

See the following sections:


- Advanced Conversation Configuration Settings, page 15-2
- Customizing the Language of System Prompts, page 15-2
- Class of Service Settings, page 15-3
- User Account and Template Settings, page 15-3
- Using the Custom Keypad Mapping Tool, page 15-5


## Advanced Conversation Configuration Settings

From the Advanced Conversation Configuration page in Unity Connection Administration, some of the systemwide conversation customizations that you can make for all users include:

- Changing the order in which Unity Connection prompts users to address and record messages.
- Changing how users confirm message addressing.
- Changing what users hear when they manage deleted messages.

See the "Changing Conversation Settings for All Users in Cisco Unity Connection 10.x" chapter for information and procedures for customizing the Unity Connection conversation from the Advanced Conversation Configuration page.

For information on all available advanced conversation configuration settings, see the "Conversation Configuration" section in the "Cisco Unity Connection 10.x Advanced Settings" chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

## Customizing the Language of System Prompts

The prompts that come with the Cisco Unity Connection system are played in different combinations in multiple places in the phone conversation.

While changing, replacing, and deleting prompts is not supported and can cause system errors, you can specify the default language in which system prompts are played to all Unity Connection users and callers. For steps on changing the default language that Unity Connection uses to play system prompts, see the "Language of System Prompts in Cisco Unity Connection 10.x" section on page 16-13.

"Language of System Prompts in Cisco Unity Connection 10.x" section on page 16-13Note that all system prompts are automatically deleted and replaced when you upgrade Unity Connection (including maintenance upgrades).

# Class of Service Settings

From the Class of Service settings page in Cisco Unity Connection Administration, conversation customizations that you can make for users include:

- Specifying call transfer and holding options.
- Enabling deleted message access.
- Determining the length of recorded names, greetings, and messages.
- Enabling features such as live reply, voice recognition, and access to external messages.
- Enabling features such as record and play video greetings for the both identified and outside callers.
- Choosing the type of message security applied to user messages.

For detailed information on conversation-related settings that can be changed for a class of service, see the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# User Account and Template Settings

Some of the conversation customizations that you can make for a user or for a template that you use to create users include:

### Caller Input Settings

- Selecting the actions that Unity Connection takes when callers enter digits during user greetings.
- Specifying keys that transfer to alternate contact numbers for a user, and optionally specifying the alternate contact numbers. (When an administrator configures a key to transfer to an alternate contact number, the user can edit the alternate contact number for the key by using the Unity Connection personal settings conversation.)
- Specifying digits that can be prepended to any number that a caller dials while listening to the greeting for the user mailbox. This option simulates shorter extensions.

### Phone Menu Settings

- Selecting the language.
- Setting the speed and volume level of prompts, recorded names, and user greetings.
- Specifying whether Unity Connection asks a user for a PIN if the user is calling from the primary extension or an alternate extension.
- Specifying how long Unity Connection waits for a user to respond to a menu, and how many times Unity Connection repeats the menu when the user does not respond.
- Choosing whether users can use the phone keypad or voice-recognition conversation when they listen to and manage their messages by phone. Note the following:
  - There are several versions of the phone keypad conversation to choose from. Each version offers menus with a unique keypad mapping. You can also specify whether users hear full or brief menus.

  - The voice-recognition conversation is a licensed feature. To use it, users must belong to a class of service that offers the license and have the feature enabled for them. Note that the touchtone conversation setting is used as a backup if the voice-recognition services are unavailable, and at any time that users choose to use the keypad rather than voice commands to interact with Unity Connection.

- Selecting the actions that Unity Connection performs when the user calls Unity Connection, including greeting the user by name, playing new messages automatically, and announcing an alternate greeting notification.
- Determining what users hear when they exit the user conversation.

#### Playback Message Settings

- Specifying the speed and volume of messages that are played by phone.
- Specifying whether Unity Connection plays the Message Type menu and message counts.
- Specifying message playback order.
- Changing the time format used for message time stamps.
- Selecting the action that Unity Connection performs when messages are played, including announcing the name and number of the sender who left a message, and whether the time stamp is played before or after the message.
- Specifying that messages are marked saved upon hang-up or disconnect.
- Specifying the length of time to skip back or ahead when rewinding or fast-forwarding messages.
- Specifying whether Unity Connection allow users to quickly listen to the messages without responding the After Message Menu options.
- Specifying whether Unity Connection asks to confirm deletions of new and saved messages.

#### Send Message Settings

- Determining whether a user can send broadcast messages to other users, or update broadcast messages.
- Specifying that Unity Connection prompts to confirm message recipients by name.
- Specifying that Unity Connection prompts to continue adding names after each recipient.
- Specifying that Unity Connection sends messages when a user hangs up or a call is disconnected.
- Determining whether users address messages to other users by entering extensions, by spelling first names, or by spelling last names.
- Enabling usage-based updates to the addressing priority list, which influences the order in which multiple matches are presented when the user addresses a message by saying a name or spelling part of a name.

For detailed information on conversation-related settings that can be changed per user, see the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

## Using the Custom Keypad Mapping Tool

The Custom Keypad Mapping tool allows you to edit the key mappings that are associated with the Custom Keypad Mapping conversations. Within each of these conversations—which are assigned to individual users or user templates on the **Phone Menu** page in Cisco Unity Connection Administration—there are eight different menus that can be customized. Changing key mappings by using this tool does not affect any of the other Cisco Unity Connection conversation versions.

You can assign any one-, two-, or three-key sequence to any defined option for the **Main** menu, the **Message Playback** menu (the message header, body and footer can be mapped separately), the **After Message** menu, the **Settings** menu, the **Message Settings** menu, and the **Personal Settings** menu. You can customize which options are voiced in each menu and the order in which they are offered. The Custom Keypad Mapping tool is accessed in the **Tools** section of Unity Connection Administration.

For more information and procedures, see the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter.

# How Users Can Customize the User Conversation in Cisco Unity Connection 10.x

Cisco Unity Connection users can customize the conversation that they hear in a number of ways. See Table 15-1 for a summary.

*Table 15-1 Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus*

| Settings That Can Be Changed by Using the Unity Connection Messaging Assistant | Settings That Can Be Changed by Using the Phone Menus |
|---|---|
| Call Holding and Screening[1]:<br>• Select how Unity Connection handles indirect calls when the user phone is busy, including placing the caller on hold, prompting the caller to hold or leave a message, and sending the caller directly to the greeting<br>• Select how Unity Connection handles indirect calls, including telling the user who the call is for, announcing that Unity Connection is transferring the call, prompting the user to accept or refuse a call, and prompting callers to say their names | Call Holding and Screening[1]:<br>• None |

*Table 15-1 Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus (continued)*

| Settings That Can Be Changed by Using the Unity Connection Messaging Assistant | Settings That Can Be Changed by Using the Phone Menus |
|---|---|
| Call Transfers[2]:<br>• Configure the three basic transfer rules: standard, alternate, and closed hours<br>• Enable or disable personal call transfer rules for each of the basic transfer rules<br>• Transfer indirect calls to an extension or send them to the user greeting<br>• Change extensions | Call Transfers[2]:<br>• Configure the three basic transfer rules: standard, alternate, and closed hours<br>• Enable or disable personal call transfer rules for each of the basic transfer rules<br>• Transfer indirect calls to an extension or send them to the user greeting<br>• Change extensions<br>• Configure alternate contact numbers for caller input keys that are assigned to the Transfer to Alternate Contact Number action |
| Caller Options:<br>• Allow callers to edit messages<br>• Allow callers to mark messages urgent | Caller Options:<br>• None |
| Phone Menu Options:<br>• Set language for Unity Connection prompts<br>• Specify whether users use the phone keypad or voice-recognition input style<br>• Set speed and volume of prompts, recorded names, and user greetings<br>• Select full or brief Unity Connection conversation menus<br>• Select the action that Unity Connection performs when the user calls Unity Connection, including greeting the user by name, and announcing the number of new messages by type<br>• Change the time format used for message time stamps<br>• Specify alternate extensions | Phone Menu Options:<br>• Select full or brief Unity Connection conversation menus |
| Greetings:<br>• Record a personal greeting<br>• Enable or disable greeting<br>• Specify an expiration date for an enabled greeting<br>• Switch between system prompt and personal greeting | Greetings:<br>• Record a personal greeting<br>• Enable or disable greeting<br>• Specify an expiration date for an enabled greeting |

*Table 15-1 Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus (continued)*

| Settings That Can Be Changed by Using the Unity Connection Messaging Assistant | Settings That Can Be Changed by Using the Phone Menus |
|---|---|
| Message Notification:<br>• Enable or disable a notification device<br>• Specify dialing or recipient options<br>• Select the types of messages and message urgency for which Unity Connection generates a notification<br>• Specify a list of message senders (by username or calling phone number) for which Unity Connection generates a notification<br>• Set up a notification schedule, and specify what happens when a device does not answer, is busy, or fails | Message Notification:<br>• Enable or disable a notification device, and change its number |
| Message Playback:<br>• Specify the speed and volume of messages that are played by phone<br>• Specify message playback order<br>• Specify whether Unity Connection plays the Message Type menu<br>• Select the action that Unity Connection performs when messages are played, including announcing the name and number of the sender who left a message, and whether the time stamp is played before or after the message<br>• Specify that messages are marked saved upon hang-up or disconnect<br>• Specify whether Unity Connection asks to confirm deletions of new and saved messages | Message Playback:<br>• Speed and volume of message as it is played |
| Message Sending and Addressing:<br>• Specify that Unity Connection prompts to confirm message recipients by name<br>• Specify that Unity Connection prompts to continue adding names after each recipient<br>• Specify that Unity Connection sends messages when users hang up or a call is disconnected<br>• Switch between addressing messages to other users by name, or by extension<br>• Specify order for addressing messages by name (last name then first name, or vice versa) | Message Addressing:<br>• Switch between addressing to other users by name or by extension (by pressing ##)[3]<br>• Review, add, or remove names in the addressing priority list[4] |

*Table 15-1 Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus (continued)*

| Settings That Can Be Changed by Using the Unity Connection Messaging Assistant | Settings That Can Be Changed by Using the Phone Menus |
|---|---|
| Personal Settings:<br>• Record a name<br>• Specify alternate names<br>• Change directory listing status<br>• Change password or PIN<br>• Add user-defined alternate extensions[5] | Personal Settings:<br>• Record a name<br>• Change directory listing status<br>• Change password or PIN<br>• Add user-defined alternate extensions[5]<br>• Edit alternate contact numbers, if an administrator has configured one or more caller input keys to transfer to an alternate contact number during the user greeting |
| Private Lists:<br>• Enter a display name<br>• Record a list name<br>• Add and delete members | Private Lists:<br>• Record a list name<br>• Add and delete members |
| Contacts:<br>• Set up contacts to use for both name dialing and call transfer rules | Contacts:<br>• None |

1. Call holding and screening options apply only to incoming calls that were routed to the user from the automated attendant or a directory handler, and not on direct calls. Holding and screening options do not apply when an outside caller or another user dials a user extension directly. In addition, holding and screening options are only available when supervised transfers are enabled. These settings apply if the user does not have personal call transfer rules enabled.
2. Call transfer options apply only to incoming calls that were routed to the user from the automated attendant or a directory handler, and not on direct calls. Transfer options do not apply when an outside caller or another user dials a user extension directly.
3. Note that this depends on whether you have enabled spelled name addressing.
4. To enable users to access the setup conversation that allows them to review, add, or remove names in the addressing priority list, the users must be assigned to a custom conversation, and you must use the Custom Keypad Mapping tool to map the Addressing Priority List conversation to a key in the Message Settings menu for that conversation.
5. Users must belong to a class of service with the Allow Users to Manage Their User-Defined Alternate Extensions option enabled. To enable users to access the phone menu conversation that allows them to review, add, or remove alternate extensions, the users must be assigned to a custom conversation, and you must use the Custom Keypad Mapping tool to map the Edit User-Defined Alternate Extensions option to a key in the Preferences Menu for that conversation.

Speed and Volume Changes Made by Users in Cisco Unity Connection 10.x, page 16-19

# Changing Conversation Settings for All Users in Cisco Unity Connection 10.x

From the **Advanced Conversation Configuration** page in Cisco Unity Connection Administration, you can make several systemwide conversation customizations that affect all users.

See the following sections for details:


- Accessibility Settings in Effect During the PIN Entry Conversation in Cisco Unity Connection 10.x, page 16-2
- Addressing Priority Lists in Cisco Unity Connection 10.x, page 16-2
- Addressing and Recording Order in Cisco Unity Connection 10.x, page 16-3
- Announcing to Users When Messages Are Marked Secure, page 16-4
- Announcing When a Message Has Been Sent to Multiple Recipients, and Listing Message Recipients, page 16-4
- Automatically Adding Alternate Extensions in Cisco Unity Connection 10.x, page 16-4
- Call Holding Wait Time in Cisco Unity Connection 10.x, page 16-5
- Warning users on Reply-All when Number of Recipients Exceeds Maximum in Cisco Unity Connection, page 16-10
- Caller Information in Cisco Unity Connection 10.x, page 16-10
- Dial Prefix Settings for Live Reply to Unidentified Callers in Cisco Unity Connection 10.x, page 16-11
- Deleting Messages in Cisco Unity Connection 10.x, page 16-12
- Language of System Prompts in Cisco Unity Connection 10.x, page 16-13
- Routing Users to the Voice-Recognition or Touchtone Conversation Style, page 16-16
- Signing In to Cisco Unity Connection 10.x from a User Greeting, page 16-17
- Requesting Users Re-Enter Only the PIN After a Failed PIN Entry in Cisco Unity Connection 10.x, page 16-18
- Saving Speed and Volume Changes Made by Users in Cisco Unity Connection 10.x, page 16-19
- Skipping Messages: Saving New Messages in Cisco Unity Connection 10.x, page 16-19

- Voice Recognition: Allowing Users to Say Their Voicemail PINs in Cisco Unity Connection 10.x, page 16-20
- Voice Recognition: Confirmation Confidence Threshold in Cisco Unity Connection 10.x, page 16-21
- Voice Recognition: Global Nickname List in Cisco Unity Connection 10.x, page 16-22
- Additional Advanced Conversation Configuration Settings in Cisco Unity Connection 10.x, page 16-23


# Accessibility Settings in Effect During the PIN Entry Conversation in Cisco Unity Connection 10.x

By default, individual user phone menu accessibility settings do not take effect until after the user is authenticated by entering the voicemail PIN. You can configure Cisco Unity Connection to apply individual user accessibility settings during the PIN collection conversation when users call from a known extension (their primary or an alternate extension) by doing the following "To Enable Accessibility Settings During the PIN Entry Conversation" procedure.

When enabled, the following accessibility settings are applied during the PIN collection conversation:

- Conversation Speed
- Conversation Volume
- Language
- Time to Wait for First Touchtone or Voice Command
- Time to Wait for Additional Key Presses When Entering Names, Extensions, and PINs

### To Enable Accessibility Settings During the PIN Entry Conversation

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check the **Apply User Accessibility Settings for Voicemail PIN Entry Conversation** check box.

**Step 3** Select **Save**.

# Addressing Priority Lists in Cisco Unity Connection 10.x

When a user attempts to address a message to a recipient by saying a name or spelling part of a name, Cisco Unity Connection may find multiple matching names. You can configure two mechanisms that direct Unity Connection to prioritize certain recipients, sorting the results and offering the names with higher weights first in the search results. Both mechanisms—a user-configurable "buddy list," and an automatic weighting of names based on usage—contribute to a single addressing priority list for the user.

You can customize how names are stored in addressing priority lists, and how long the names are stored.

### To Change How Names Are Stored in User Addressing Priority Lists

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Maximum Age of Names in Addressing Priority Lists** field, enter the number of days that a name can remain on the addressing priority list for a user before being automatically removed if the user has not recently addressed a message to the name. (The default setting is 90 days.)

**Step 3** In the **Maximum Number of Names in a User's Addressing Priority List** field, enter the number of names that are stored in the addressing priority list for each user. (The default setting is 100 names.)

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

# Addressing and Recording Order in Cisco Unity Connection 10.x

The Cisco Unity Connection standard conversation can be customized to change the order in which Unity Connection prompts users to address and record when they send or forward messages to other users or distribution lists. By default, when a user sends or forwards a message, Unity Connection first prompts the user to record the message or to record an introduction for a forwarded message, and then prompts the user to address the message.

You can customize the user conversation so that Unity Connection prompts users to address a message before recording the message or an introduction. This setting change is applied systemwide to all users. You cannot make the change for an individual user or a specific group of users. Finally, note that you cannot change the order in which Unity Connection prompts users to address and record when they reply to messages; Unity Connection always prompts users to record a reply before allowing them to add additional recipients.

### To Change the Order of Addressing and Recording When Users Send Messages

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check or uncheck the **Address Message Before Recording** check box, depending on how you want to change this setting:

- **Check box checked**—When users send or forward messages to other users or distribution lists, Unity Connection prompts them to address the message first and then record it.
- **Check box not checked**—When users send or forward messages to other users or distribution lists, Unity Connection prompts them to record the message first and then address it. (This is the default setting.)

**Step 3** Select **Save**.

# Announcing to Users When Messages Are Marked Secure

When the Announce Secure Status in Message Header check box is checked on the **System Settings > Advanced Settings > Conversation Configuration** page, Cisco Unity Connection plays a prompt to the user before playing a secure message, announcing that it is a secure message. When this check box is not checked, Unity Connection does not announce the secure status of a message to users. By default, the check box is checked.

If you have configured Unity Connection such that all messages left by both users and outside callers are configured to be secure, consider unchecking this check box so that users do not hear the secure message prompt before every message that they listen to.

# Announcing When a Message Has Been Sent to Multiple Recipients, and Listing Message Recipients

### Announcing When a Message Had Been Sent to Multiple Recipients

The Cisco Unity Connection conversation can be customized so that when a message has been sent to multiple recipients, Unity Connection will announce that fact to the user before playing the message.

By default, this setting is not enabled. To enable the setting for users of both the voice-recognition and touchtone conversations, check the **Announce in Message Header Whether Message Has Multiple Recipients** check box on the **System Settings > Advanced > Conversation Configuration** page.

### Listing Recipients While Listening to Messages

Unity Connection can also be customized so that users can hear a list of all of the recipients of a message. By default, users who are enabled for voice-recognition can hear a list of message recipients by saying "list recipients" while listening to the message header, body, footer, or after-message prompts. By default, this functionality is not enabled for the touchtone conversation, and must be configured by using the Custom Keypad Mapping tool. Depending on how you configure the key mapping, users can hear the list of message recipients when they press the applicable key while listening to the message header, body, footer, or after-message prompts. For detailed information on using the Custom Keypad Mapping tool, see the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter.

# Automatically Adding Alternate Extensions in Cisco Unity Connection 10.x

When a user signs in from a phone number other than a primary extension or alternate extension, Cisco Unity Connection adds the number to the calling party ID (CPID) history of the user. If the user signs in from the number five times within 30 days, Unity Connection offers the option of adding it as an alternate extension. When a number is added as an alternate extension, the user can sign in to Unity Connection from the number without having to enter a user ID (the primary extension). If the user chooses not to add the number as an alternate extension, Unity Connection does not offer the option again for that number.

This functionality is available to users who belong to a class of service with the **Allow Users to Manage Their User-Defined Alternate Extensions** option enabled.

The restriction table named User-Defined and Automatically-Added Alternate Extensions, the restriction tables is named Excluded Extensions for Automatically Added Alternate Extensions) restricts numbers from being offered as alternate extensions. For example, you might block a lobby or conference room extension in the restriction table so that users who frequently sign in to Unity Connection from such shared phones are not offered the alternate extension option. The same restriction table also restricts the numbers that users can use to create alternate extensions for themselves through interfaces such as the Cisco Personal Communications Assistant or via an API call.

You can adjust the number of times a user must sign in from a phone number before Unity Connection offers the option to add the number as an alternate extension. You can also change the number of consecutive days within which Unity Connection considers the sign-in count before offering the alternate extension option.

#### To Adjust Settings to Automatically Add Alternate Extensions

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Sign-in Count for a Number Before It Is Offered as an Alternate Extension** field, enter a number between 2 and 60.

**Step 3** In the **Consecutive Days to Count Sign-in for a Number**, enter a number between 7 and 60 days.

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

# Call Holding Wait Time in Cisco Unity Connection 10.x

With call holding, when the phone is busy, Cisco Unity Connection can ask callers to hold. Unity Connection manages each caller in the queue according to the settings that you configure.

You can change the setting for the wait time between call transfer attempts (the default value is 5 seconds), and for the maximum number of call transfer attempts that are allowed (the default value is 5 attempts). To obtain the call holding queue wait time for the first caller in the queue, Unity Connection multiplies the values of the two settings. For example, if both keys were set to a value of 10, the call holding queue wait time would be 100 seconds (a wait time of 10 seconds x 10 call transfer attempts). The first caller on hold in the call holding queue hears a series of holding tones approximately every five seconds. Subsequent callers in the queue for the same extension will hear music on hold that is generated by Cisco Unity Connection system prompts.

#### To Add or Change Call Holding Wait Time

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Maximum Call Transfer Attempts Allowed** field, enter a number between 0 (zero) and 30. We recommend a value between 2 and 10, as increasing this setting decreases the frequency at which Unity Connection asks whether the caller wants to continue to hold. (The default setting is 5 attempts.)

**Step 3** In the **Wait Time in Seconds Between Call Transfer Attempts** field, enter a number between 1 and 60 seconds. We recommend a value between 5 and 15 seconds, as a value outside of this range could prevent Unity Connection from functioning as designed. (The default setting is 5 seconds.)

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

# Announcing Message Status on Reply or Reply-All in Cisco Unity Connection

Cisco Unity Connection announces message status to the users when they reply or reply-all to a message. By default, when a user replies or reply-all to a message, Unity Connection will not announce any message status.

The following are the message status when users reply or reply-all to a message:

- Urgent
- Private
- Private and Secure

This setting for reply or reply-all to a message can be configured for both touchtone and voice-recognition conversation users.

Do the following Procedure

### To Announce the Message Status

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check the **Announce Message Status to User(s) while Replying** check box. (The default setting is check box not checked)

**Step 3** Select **Save**.

See Table 16-1, when the administrator enables or disables the **Announce Message Status to User(s) while Replying** option.

*Table 16-1 Message Status Announcement*

| User Action | Announce Message Status to User(s) while Replying | Expected Behavior |
|---|---|---|
| Reply to a message | Disabled | Unity Connection will not announce message status |
| Reply-all to a message | Disabled | Unity Connection will not announce message status |
| Reply to a message | Enabled | Unity Connection will announce the status of the message |
| Reply-all to a message | Enabled | Unity Connection will announce the status of the message |

For more information on message status announcement, see the Conversation Configuration section of the Cisco Unity Connection 10.x Advanced Settings chapter.

# Announcing Recipient List on Reply or Reply-All in Cisco Unity Connection 10.x

When a message is sent to multiple recipients and/or distribution lists, recipients have the option to reply-all. Cisco Unity Connection announces the recipient list to the users when they reply-all to a message whose number of recipients is less than the number specified in the Maximum Number of Recipients Before Reply-all Warning field. By default, when a user replies to all recipients of a message, Unity Connection will not announce any recipient list on reply-all. The setting for reply-all recipients of a message can be configured for both touchtone and voice-recognition conversation users.

**Note** Unity Connection warns the user (default behavior), when a user reply-all to a message whose number of recipients is greater than or equal to the number specified in the Maximum Number of Recipients Before Reply-all Warning field.

Unity Connection 10.0(1) and later plays only the recipient name, when the user reply to a message. Reply to a message is irrespective of the value mentioned in the Maximum Number of Recipients Before Reply-all warning field.

### To Announce the Recipient List

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the Conversation Configuration page, check the Announce Recipients list to User(s) while Replying check box. (The default setting is check box not checked).

**Step 3** Select **Save**.

See Table 16-2, when the administrator enables or disables the Announce Recipients list to User(s) while Replying option.

*Table 16-2 Recipient List Announcement*

| User Action | Announce Recipients list to User(s) while Replying | Expected Behavior |
|---|---|---|
| Reply to a message | Disabled | Unity Connection will not announce the recipient name |
| Reply-all to a message | Disabled | Unity Connection will not announce the recipient list |

| User Action | Announce Recipients list to User(s) while Replying | Expected Behavior |
|---|---|---|
| Reply to a message | Enabled | Unity Connection will announce the recipient name |
| Reply-all to a message | Enabled | Unity Connection will announce the recipient list |

**Note** The **Announce Recipients list to User(s) while Replying** setting only applicable when the number of recipients is less than the number specified in the **Maximum Number of Recipients Before Reply-all Warning** field

For more information on message status announcement, see the Conversation Configuration section of the Cisco Unity Connection 10.x Advanced Settings chapter.

# Announcing Message Status on Reply or Reply-All in Cisco Unity Connection

Cisco Unity Connection announces message status to the users when they reply or reply-all to a message. By default, when a user replies or reply-all to a message, Unity Connection will not announce any message status.

The following are the message status when users reply or reply-all to a message:

- Urgent
- Private
- Private and Secure

This setting for reply or reply-all to a message can be configured for both touchtone and voice-recognition conversation users.

### To announce the Message Status

**Step 1** In Cisco Unity Connection Administration, expand **System Settings** > **Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check the **Announce Message Status to User(s) while Replying** check box. (The default setting is check box not checked).

**Step 3** Select **Save**.

See Table 16-3, when the administrator enable or disable the **Announce Message Status to User(s) while Replying** option.

*Table 16-3 Message Status Announcement*

| User Action | Announce Message Status to User(s) while Replying | Expected Behavior |
|---|---|---|
| Reply to a message | Disabled | Unity Connection will not announce message status. |
| Reply-all to a message | Disabled | Unity Connection will not announce message status. |
| Reply to a message | Enabled | Unity Connection will announce the status of the message. |
| Reply-all to a message | Enabled | Unity Connection will announce the status of the message. |

# Announcing Recipient List on Reply or Reply-All in Cisco Unity Connection

When a message is sent to multiple recipients and/or distribution lists, recipients have the option to reply-all. Cisco Unity Connection announces the recipient list to the users when they reply-all to a message whose number of recipients is less than the number specified in the **Maximum Number of Recipients Before Reply-all Warning** field. By default, when a user replies to all recipients of a message, Unity Connection will not announce any recipient list on reply-all. The setting for reply-all recipients of a message can be configured for both touchtone and voice-recognition conversation users.

**Note** Unity Connection warns the user (default behavior), when a user reply-all to a message whose number of recipients is greater than or equal to the number specified in the **Maximum Number of Recipients Before Reply-all Warning** field.

Cisco Unity Connection 10.0(1) and later plays only the recipient name, when the user reply to a message. Reply to a message is irrespective of the value mentioned in the **Maximum Number of Recipients Before Reply-all warning** field.

### To announce the Recipient List

**Step 1** In Cisco Unity Connection Administration, expand **System Settings** > **Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check the **Announce Recipients list to User(s) while Replying** check box. (The default setting is check box not checked).

**Step 3** Select **Save**.

See Table 16-4, when the administrator enable or disable the **Announce Recipients list to User(s) while Replying** option.

*Table 16-4 Message Status Announcement*

| User Action | Announce Message Status to User(s) while Replying | Expected Behavior |
|---|---|---|
| Reply to a message | Disabled | Unity Connection will not play the recipient name. |
| Reply-all to a message | Disabled | Unity Connection will not play the recipient list. |
| Reply to a message | Enabled | Unity Connection will play the recipient name. |
| Reply-all to a message | Enabled | Unity Connection will play the recipient list. |

# Warning users on Reply-All when Number of Recipients Exceeds Maximum in Cisco Unity Connection

When a message is sent to multiple recipients and/or distribution lists, recipients have the option to reply-all. Cisco Unity Connection warns users when they reply-all to a message whose number of recipients is equal to or exceeds the number specified in the **Maximum Number of Recipients Before Reply-all Warning** field.

By default, when a user replies to all recipients of a message, Unity Connection will not issue any warnings on reply-all.

**Note** The setting for reply-all recipients of a message can be configured for both touchtone and voice-recognition conversation users.

### To set the maximum number of recipients

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Maximum Number of Recipients Before Reply-all Warning** field, enter the maximum number of recipients and/or distribution lists. (The default setting is 0 recipients)

**Step 3** Select **Save**.

# Caller Information in Cisco Unity Connection 10.x

The Cisco Unity Connection user conversation can be customized so that it provides users with additional information about each caller who left a message, before it plays the message. See Table 16-5.

*Table 16-5 Caller Information That Cisco Unity Connection Can Offer Before Message Playback*

| For Messages Left by This Type of Caller | Message Type | Cisco Unity Connection Plays This by Default | Cisco Unity Connection Plays This When Additional Caller Information Is Offered |
|---|---|---|---|
| Identified user (including call handlers) | Voice, receipts | The recorded name of the user (or call handler). If the user (or call handler) does not have a recorded name, Unity Connection uses Text to Speech to play the display name. If the user does not have a display name, Unity Connection plays the primary extension instead. | Both the recorded name (if available) and the primary extension (if available) before playing the message.<br>If the user (or call handler) does not have a recorded name, Unity Connection uses Text to Speech to play the display name of the user (or call handler) instead. |
| Outside caller | Voice | The message, without announcing who it is from or playing the phone number of the caller first. | The phone number (if available) of the caller before playing the message. |

If you choose to provide Unity Connection users with additional caller information before message playback, consider the following requirements:

- Users hear sender information before Unity Connection plays each message only if their accounts are configured to play it. Either a Unity Connection administrator or a user can specify message playback preferences. (Unity Connection administrators specify whether users hear sender information before message playback on the Edit Playback Message Settings page for a user or user template in Cisco Unity Connection Administration, while users can specify their own message playback preferences in the Unity Connection Messaging Assistant.)
- In addition, to allow Unity Connection to provide the phone number (ANI or caller ID) information for outside callers, your phone system must support sending such information to Unity Connection. (See your phone system documentation for more information.) When Unity Connection receives ANI information on a caller, it makes use of the valid numbers only, and ignores any other characters that the phone system sends.

For instructions on changing these settings for individual users or a specific group of users, see the "What Cisco Unity Connection Plays Before and After Each Message" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Dial Prefix Settings for Live Reply to Unidentified Callers in Cisco Unity Connection 10.x

When live reply is enabled, users who are listening to messages by phone can reply to a message by having Cisco Unity Connection call the sender. In the user class of service settings, you can specify whether users can return calls to senders of messages only if they are also Unity Connection users, or if they can return calls to messages from both users and unidentified callers (outside callers or users who are forwarded to Unity Connection but who cannot be identified by the calling extension).

When a user attempts to reply by calling an unidentified caller, Unity Connection checks the calling number provided by the phone system in the Automatic Number Identification (ANI) string against the transfer restriction table that is associated with the user class of service. If the number is allowed, Unity Connection returns the call by performing a release transfer to the ANI.

To configure a prefix that Unity Connection applies to all ANI strings of sufficient length before performing live replies to unidentified callers, do the following procedure.

**To Change Dial Prefix Settings for Live Reply to Unidentified Callers**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Dial Prefix for Live Reply to Unidentified Callers** field, enter a trunk access code or other identifying ID that the phone system requires to process the number correctly.

This setting specifies a prefix that Unity Connection applies to the ANI when performing a live reply to an unidentified caller, if the caller ANI is at least as long as the **Minimum Number of Digits Required for Prepending Live Reply Dial Prefix** setting.

**Step 3** In the **Minimum Number of Digits Required for Prepending Live Reply Dial Prefix** field, enter the minimum number of digits in the ANI string required for Unity Connection to prepend the value specified in the **Dial Prefix for Live Reply to Unidentified Callers** setting to the ANI when performing a live reply to an unidentified caller. A value of 0 means that Unity Connection never prepends digits when performing live reply to unidentified callers. (The default setting is 0 digits.)

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

# Deleting Messages in Cisco Unity Connection 10.x

From the **System Settings > Advanced > Conversations** page, you can customize the standard conversation to change what users hear when they manage their deleted messages in the following ways:

- Change how Cisco Unity Connection permanently deletes multiple deleted messages. By default, when users press keys from the Main menu to permanently delete multiple deleted messages at once, Unity Connection allows them to choose which messages they want to delete; users can either delete their deleted voice messages or delete all of their deleted messages.

  As alternatives to the default, you can specify that Unity Connection does not prompt users to choose, and instead permanently deletes the type of messages that you specify: either deleted voice messages or all deleted messages (voice and email, as applicable). To set up either alternative, change the **Multiple Message Delete Mode** setting by entering one of the following values:

  - **1**—Users choose which messages are deleted; Unity Connection prompts them: “To delete only your voice messages, press 1. To delete all messages, press 2.” (Default setting)
  - **2**—Unity Connection does not prompt users to choose which messages to delete; instead, Unity Connection deletes all of their deleted voice messages.
  - **3**—Unity Connection does not prompt users to choose which messages to delete; instead, Unity Connection deletes all of their deleted messages (voice messages, receipts, and email messages, as applicable).

- Enable Unity Connection to request confirmation from users before proceeding with a permanent deletion of a single deleted message. (To permanently delete a deleted message, users must belong to a class of service that allows them to retain and review deleted messages.) By default, when users permanently delete a deleted message as they review deleted messages by phone, Unity Connection does not ask them to confirm the deletion.

  You can enable Unity Connection to request confirmation from users before proceeding with the deletion. To do so, check the **Confirm Deletion of Deleted Messages** check box.

# Language of System Prompts in Cisco Unity Connection 10.x

Phone languages are the languages in which Cisco Unity Connection can play system prompts to users and callers. You specify a system default phone language, and you can also customize the language setting for individual Unity Connection components without changing the default language settings for the rest of the system.

The phone language setting is available for the following Unity Connection components: user accounts, routing rules, call handlers, interview handlers, and directory handlers. For each of these entities, you specify a phone language in Cisco Unity Connection Administration, or you can set the entities to inherit language from the caller.

**Note** The phone language setting does not apply to the prompts that Unity Connection plays when callers are using the voice-recognition conversation. Voice-recognition prompts are always played in English-United States, regardless of the installed languages or the system configuration.

With the **Inherit Language from Caller** setting, Unity Connection determines the phone language to use on a per-call basis, depending on how the call is processed. For example, you can set up a call handler with the Inherit setting, and also set it up to receive calls from two different routing rules, each with a different language setting. (For example, one routing rule could be set up with a French language setting, while the second routing rule could be set to German.) In this situation, the language in which Unity Connection plays the call handler system prompts depends on which rule routed the call. However, note that if every component in your system that processes a call has been set with **Inherit Language from Caller**, Unity Connection plays the system prompts in the default phone language, because in effect none of the components have been set to a specific language.

For multilingual systems, it is possible to enable users to record greetings in each language installed on the Unity Connection server, independent of the system default language, by setting the **Inherit Language from Caller** setting. In general, the language in which recorded greetings are played depends on what is selected for the **Language That Callers Hear** setting on the **Message** Settings page for the user:

| | |
|---|---|
| **Use System Default Language** | Greetings are played and recorded in the language selected as the system default. |
| **Inherit Language From Caller** | Unity Connection users are able to record greetings in each language installed on the Unity Connection server. |
| **A specific language** | Greetings are played and recorded in the language selected from this menu. |

For information on changing message settings for a user or template, see the "Phone Language That Users and Callers Hear" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

**To Change the Default Language for System Prompts**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **General Configuration** page, in the **System Default Language** list, select the language that Unity Connection uses as the default language for playing system prompts.

**Step 3** Select **Save**.

**Step 4** Restart the **Voice Processing** server role for your changes to take effect.

# Allowing Users to Playback Video Greetings in Cisco Unity Connection 10.x

Cisco Unity Connection 10.0(1) facilitates the user to playback video greetings for both the identified and outside callers using a video endpoint. For more information on video greetings, see "Overview of Video Greetings in Cisco Unity Connection" section on page 11-1 and "Enabling a User Greeting" section on page 4-62.

Unity Connection allows users to playback video greetings using telephone user interface (touchtone conversation). You can enable or disable the video greeting settings using both the telephone user interface and Cisco Unity Connection Administration interface. For more information on playback of video greeting using telephone user interface, see the "Managing Personal Greetings" section in the *User Guide for the Cisco Unity Connection Phone Interface*.

To allow playback of video greetings for each user, enable the **Callers See** settings in Cisco Unity Connection Administration. To enable the Callers See settings navigate to **Users > Edit User> Greetings> Edit Greeting page> Callers See> My Personal Recording**. Unity Connection facilitates you to play six personal video greetings. However, error greetings are played audio only. For more information on Callers See and Callers Hear sections, see the "Edit Greeting" Section of the Cisco Unity Connection 10.x User Settings chapter in the *Interface Reference Guide for Cisco Unity Connection Administration*.

In case of an audio call, consider the scenarios in the table below, when a user enable or disable the Callers See or Callers Hear settings.

| Existing Greetings in Cisco Unity Connection | Callers Hear Settings (My Personal Recording) | Callers See Settings (My Personal Recording) | Type of Greeting that Cisco Unity Connection play |
|---|---|---|---|
| • Audio Greeting<br>• Video Greeting<br><br>**Note** When a user record a new audio greeting, it is replaced by the last audio greeting in the system. | Enabled | Disabled | If the user calls using either a video or an audio phone, the audio greeting enabled in the Callers Hear section is played. |
| • Audio Greeting<br>• Video Greeting | Enabled | Enabled | • If the user calls using a video phone, the audio part of the video greeting is played.<br>• If the user calls using an audio phone, the audio greeting enabled in the Callers Hear section is played. |
| • Audio Greeting only | Enabled | Enabled | If the user calls using either a video or an audio phone, the audio greeting enabled in the Callers Hear section is played. |

In case of a video call, consider the scenarios in the table below, when a user enable or disable the Callers See or Callers Hear settings.

| Existing Greetings in Cisco Unity Connection | Callers Hear Settings (My Personal Recording) | Callers See Settings (My Personal Recording) | Type of Greeting that Cisco Unity Connection play |
|---|---|---|---|
| • Audio Greeting<br>• Video Greeting | Enabled | Disabled | If the user calls using either a video or an audio phone, the audio part of the video greeting is played. |
| • Audio Greeting<br>• Video Greeting | Enabled | Enabled | • If the user calls using a video phone, the video greeting enabled in the Callers See section is played.<br>• If the user calls using an audio phone, the audio part of the video greeting is played. |

Note the following:

- If a user records a video greeting, Cisco Unity Connection enables the "My Personal Recording" option in the Callers See section.
- If the Callers See settings are disabled before a user records a video greeting, then to play video greetings the user needs to enable the "The My Personal Recording" option in the Callers See section.

# Routing Users to the Voice-Recognition or Touchtone Conversation Style

There are multiple ways to route users to either the touchtone or voice-recognition conversation style:

- Set up separate phone numbers for each of the conversation styles, and then distribute the different call-in numbers to users, and/or set the user devices to automatically dial the applicable phone number. Depending on which number the user calls to sign in to Cisco Unity Connection, the user will be routed either to the touchtone or voice-recognition conversation. This approach is particularly useful in cases where users prefer different conversation styles based on the device with which they place the call. For example, when calling in from a mobile phone, the user may prefer the touchtone conversation because background noise picked up on the mobile phone interferes with the voice-recognition conversation. But when calling in from an office phone, the user prefers the voice-recognition conversation.

  To do this, set routing rule conditions that are associated with the phone number by entering the applicable information on the routing rule condition page. Then in the Send Call To field on the routing rule page, specify that when the conditions are met, the call launches the applicable conversation. When the conditions for this routing rule are met, and the user subsequently signs in on that call, the user hears the selected conversation.

**Note** You can send the call to other conversations in addition to the voice-recognition and touchtone conversation styles. For more information, see the "Edit Direct Routing Rule" or "Edit Forwarded Routing Rule" section in the "Cisco Unity Connection 10.x Call Management Settings" chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

- Make use of the functionality that allows users to toggle between the touchtone and voice-recognition conversations at any time from the main menu:
  - Notify users that while listening to the voice-recognition conversation, they can press "9" to switch immediately to the touchtone conversation. Likewise, while listening to the touchtone conversation, users can press "9" to switch immediately to the voice-recognition conversation.

**Tip** When users press "9" to switch conversations, they are asked to confirm the switch. If they prefer to bypass being asked to confirm, they can press "91," effectively answering the confirmation request before it is asked.

In addition, at any time while signed in to Unity Connection, users who are assigned to the voice-recognition conversation can say "touchtone conversation" to immediately switch to the touchtone conversation.

- If you prefer a key setting different from "9," use the Custom Keypad Mapping tool to change the key presses that toggle users from the touchtone and voice-recognition conversations, and then notify users of the key presses you have set. The option to change is the "Toggle between touchtone and voice-recognition conversations" option on the Main Menu tab. (For information on using the Custom Keypad Mapping tool, see the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter.)

# Signing In to Cisco Unity Connection 10.x from a User Greeting

Caller input settings allow you to specify how users sign in to Cisco Unity Connection when they are listening to a user greeting. By using the caller input settings you can specify which keys users can press to interrupt a user greeting so that they can sign in to Unity Connection, and what users hear after Unity Connection prompts them to sign in.

You specify caller input settings on the user template and on individual user pages in Cisco Unity Connection Administration. **Caller input** settings work for a particular greeting only when the Ignore Additional Input check box is not checked on the applicable **Greetings** page for the user template or individual user in Connection Administration.

By default, Unity Connection is set up so that users hear the Unity Connection Sign-In conversation, which prompts them for their ID and PIN when they press * during any user greeting—either their own or another user greeting. As an alternative, you can accommodate users who want an easier way to sign in from their own greeting by offering the Easy Sign-In conversation, which prompts users only for a PIN.

Table 16-6 summarizes the options available to you for specifying how users sign in to Unity Connection from their own greeting or from another user greeting.

***Table 16-6 Summary of Caller Input Options Available for Specifying How Users Sign In to Cisco Unity Connection from User Greetings***

| Conversation | Description | Use | Best Practice |
|---|---|---|---|
| Sign-In | Prompts users to enter an ID and PIN when they press * during any user greeting.<br>Enabled by default. | To avoid leaving a message as an unidentified caller, users can sign in to Unity Connection from another user greeting when they call the user from a phone that is not associated with their account. (Unity Connection users cannot reply to messages from unidentified callers.) | Continue to offer the Sign-In conversation.<br>If you are considering reassigning the key used to access the Sign-In conversation, consider that users also access the Sign-In conversation by pressing * from the Opening Greeting. |

*Table 16-6 Summary of Caller Input Options Available for Specifying How Users Sign In to Cisco Unity Connection from User Greetings (continued)*

| Conversation | Description | Use | Best Practice |
|---|---|---|---|
| Easy Sign-In | Prompts users to enter a PIN when they press a key during any user greeting.<br>Disabled by default. (No key is mapped to the Easy Sign-In conversation.) | Users can dial their extensions and sign in quickly without having to remember the pilot number to access Unity Connection by phone.<br>Users may prefer Easy Sign-In to the Sign-In conversation because it saves them from having to re-enter an extension during the sign-in process. Note that Unity Connection uses the calling extension (rather than the dialed extension) to determine which mailbox the user is trying to sign in to. | Provide Easy Sign-In to users who want a faster way to sign in from their own greeting or to accommodate users who are accustomed to another voice messaging system.<br>Keys 1–9 are unmapped, and are therefore good choices for assigning to the Easy Sign-In conversation. Consider the following if you are thinking of using the *, 0, or # key instead:<br>• Avoid reassigning the * key so that you can continue to offer the Sign-In conversation.<br>• The # key is already set up to skip greetings. It is also the key that users use to skip ahead throughout the Unity Connection conversation.<br>• The 0 key is already set up to send callers to the Operator call handler. |

# Requesting Users Re-Enter Only the PIN After a Failed PIN Entry in Cisco Unity Connection 10.x

When users call Cisco Unity Connection from their extensions or alternate extensions, Unity Connection asks only for a PIN to authenticate the user. By default, if a user enters an incorrect PIN, Unity Connection asks for both the user ID and PIN on subsequent attempts to sign in. Alternatively, you can configure Unity Connection to ask for only the user PIN on subsequent attempts to sign in.

Note that the default behavior has been set for security reasons; asking for only the user PIN gives hackers confirmation that the user ID was legitimate.

### To Configure Cisco Unity Connection to Ask Only for the User PIN After a Failed PIN Entry

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, uncheck the **Request Entry of User ID After Failed PIN Entry from Known Extension** check box.

**Note** This setting applies only to calls from extensions that are associated with a user. It does not apply when users attempt to sign in manually from an unknown number.

**Step 3** Select **Save**.

# Saving Speed and Volume Changes Made by Users in Cisco Unity Connection 10.x

Speed and volume changes that users make while listening to messages or to the Cisco Unity Connection conversation can be saved as new default settings for the user.

**Note** The voice-recognition conversation is the only conversation that allows users to change the Unity Connection conversation speed or volume by phone.

Do the following procedure to specify whether speed and volume changes made by users are saved by Unity Connection.

### To Specify Whether Cisco Unity Connection Saves Speed and Volume Changes Made by Users

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check or uncheck the **Save Speed and Volume Changes Made by User** check box:

- When this check box is checked, speed and volume changes that the user makes while listening to messages or to the Unity Connection conversation will be saved as new default settings for the user.
- When this check box is not checked, any speed and volume changes that the user makes while listening to messages are in effect for all the messages in that phone session. Any speed and volume changes that the user makes while listening to the Unity Connection conversation are in effect only for the duration of that phone session.

**Step 3** Select **Save**.

# Skipping Messages: Saving New Messages in Cisco Unity Connection 10.x

You can customize how Cisco Unity Connection handles new messages that users skip during message playback. By default, when users press # to skip a new message during message playback, Unity Connection saves the message as new. This means that when users call Unity Connection to check messages, the skipped message remains in the list of new messages that Unity Connection plays. In addition, message waiting indicators (MWI) on user phones remain lit as long as there are new messages.

Alternatively, you can configure Unity Connection to save new messages that users skip by pressing # during message playback as saved messages rather than as new messages. Users in your organization may prefer this so that when they call Unity Connection to check for new messages, they hear only newly-arrived messages, and not the messages that they skipped earlier. Users can then rely on their MWIs to determine when a new message arrives.

A change to the message playback setting is applied systemwide to all users. You cannot make the change for an individual user or a specific group of users.

### To Change How Cisco Unity Connection Handles Messages That Users Skip by Pressing # During Message Playback

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check the **Treat Skipped Messages as Saved** check box to specify that messages that users skip by pressing # during message playback are kept as saved messages.

**Step 3** Select **Save**.

# Voice Recognition: Allowing Users to Say Their Voicemail PINs in Cisco Unity Connection 10.x

You can customize the Cisco Unity Connection sign-in process so that voice recognition users can say the digits in their voicemail PINs to sign in when calling Unity Connection from their primary or alternate extensions. Unity Connection attempts to match the spoken digits to the user voicemail PIN as an alternative to entering the digits on the phone keypad; it does not attempt to recognize the individual voice print of the user or otherwise apply biometrics to the sign-in process.

In order to use the voicemail PIN feature, a user must be calling from the primary extension or an alternate extension, the extension must be configured to use the voice-recognition input style, and the language of the call must be set to English (United States) when the user reaches the Attempt Sign-In conversation.

**Caution** The spoken digits are transmitted as unencrypted text by the Unity Connection Voice Recognizer to be authenticated by Unity Connection, and can appear as plain text in diagnostic log files.

If desired for security reasons, users can continue to use the phone keypad to enter the PIN rather than saying the digits, even when this feature is enabled. However, users cannot mix voice and phone keypad keys for PIN entry—if the user starts to use the keypad to enter the PIN, voice recognition is disabled until the user signs in successfully. Also, after a single unsuccessful attempt to say the voicemail PIN, the user must use the keypad to retry the PIN entry.

### To Allow Voice Recognition Users to Say Their Voicemail PINs

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, check or uncheck the **Allow Voice Recognition Users to Speak Their Voicemail PINs** check box, depending on how you want to change the setting:

- **Check box checked**—Voice recognition users can enter their voicemail PINs either by saying the digits in the PIN, or by using the phone keypad. Unity Connection allows users to say their PINs only when they are calling from their primary extension or one of their alternate extensions.
- **Check box not checked**—Voice recognition users must enter their voicemail PINs by using the phone keypad. (This is the default setting.)

**Step 3** Select **Save**.

# Voice Recognition: Confirmation Confidence Threshold in Cisco Unity Connection 10.x

When voice-recognition users choose to exit the system, send a message, delete a message, or cancel an action, Cisco Unity Connection may or may not prompt them to confirm that they want to perform this task ("Are you sure that you want to exit?"), depending on whether or not their voice command was clearly recognized by the system.

There are a variety of factors that may influence how well the voice-recognition system "hears" a voice command: phone line quality, background noise, or how quickly or slowly a user speaks.

You use the **Voice Recognition Confirmation Confidence Threshold** setting to adjust the likelihood that Unity Connection prompts voice recognition users to confirm their intentions. The range of valid entries for the **Voice Recognition Confirmation Confidence Threshold** is 0 to 100; the default value is 60, which should reliably filter out most errors and provide confirmation when necessary for most systems. For example, if users complain that the system mistakenly hears them say "cancel" or "hang up," you may want to try increasing this setting to a value of 75 to prevent users from accidentally committing actions that they did not intend. Alternatively, if users complain that the system prompts for confirmation too frequently, try lowering this setting to 55.

A realistic range of values for this setting is 30 to 90, as setting this value to 0 always disables confirmation and setting it to 100 always enables it. If this value is set too low, the system may improperly recognize and act on commands, resulting in the accidental deletion of messages or exiting users from the system before they are ready to hang up.

It is important to note that for some tasks—for example, emptying the Deleted Items folder—Unity Connection always prompts for confirmation regardless of the **Voice Recognition Confirmation Confidence Threshold** setting. Likewise, Unity Connection never prompts for confirmation for tasks—such as playing messages—that do not result in user issues if the command is misunderstood by the system.

### To Set the Confirmation Confidence Threshold

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Conversations**.

**Step 2** On the **Conversation Configuration** page, in the **Voice Recognition Confirmation Confidence Threshold** field, enter a new value.

You can enter a value from 0 to 100; the default value is 60.

**Step 3** Select **Save**.

# Voice Recognition: Global Nickname List in Cisco Unity Connection 10.x

The Global Nickname list is a comprehensive list of common nicknames that Cisco Unity Connection considers when a caller uses voice recognition to place a call or to address messages. For example, Unity Connection considers "Bill," "Billy," and "Will" to be nicknames for the name "William."

If a user has an uncommon name or if others know the user by a different name (for example, a maiden name) consider adding these alternate names for the user. Alternate names improve the likelihood of Unity Connection placing a call when callers ask for the user by name. You can add and remove nicknames from this list by using Cisco Unity Connection Administration.

### To Add Nicknames to the Global Nickname List

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Global Nicknames**.

**Step 2** On the **Search Global Nicknames** page, select **Add New**.

**Step 3** On the **New Global Nickname** page, in the **Proper Name** field, enter the name that you want to appear in the **Global Nickname** list.

**Step 4** In the **Nickname** field, enter the nickname for this name.

**Step 5** Select **Save**.

**Step 6** If there is more than one nickname, select **Add New**, replace the **Must-Be-Unique-Nick-Name** text in the new field with the next nickname and select **Save**.

**Step 7** Repeat Step 6 until all information has been added.

### To Edit the Global Nicknames List

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Global Nicknames**.

**Step 2** On the **Search Global Nicknames** page, find the nickname you want to edit.

**Note** If the nickname does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** To delete a proper name and its associated nicknames, check the check box next to the name in the **Global Nickname** list, and select **Delete Selected**.

**Step 4** Select the proper name to edit the nicknames that are associated with it. Do any of the following:

- In the **Proper Name** field, enter changes to the name.
- If you want to delete a nickname, check the check box next to the name, and select **Delete Selected**.
- Select **Add New** to add a new nickname, and enter the applicable information.

**Step 5** Select **Save**.

# Additional Advanced Conversation Configuration Settings in Cisco Unity Connection 10.x

The following customizations and features are also available on the **Advanced Conversation Configuration** page in Cisco Unity Connection Administration. For configuration information, see the "Conversation Configuration" section in the "Cisco Unity Connection 10.x Advanced Settings" chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x* (unless otherwise indicated), at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

- Remote Port Status Monitor settings
- Disable Identified User Messaging Systemwide
- Enable Go to Message
- Deactivate Notification Device settings
- Disable Message Summary on Replay
- Disable Spelled Name Searches
- Play Receipt Reason Code
- System Transfers: Confirm Number Before Transfer
- Prompt User to Record an Introduction when Forwarding Messages
- Skip Recording of Greeting During Enrollment
- Time to Wait Between Spoken Words (in Milliseconds)
- Maximum Call Transfer Attempts Allowed
- Maximum number of recipients Before Reply-All Warning.
- Wait Time in Seconds Between Call Transfer Attempts
- Require Users to Record Names at Enrollment
- System Broadcast Message settings (see the "Changing Broadcast Message Administrator Defaults in Cisco Unity Connection 10.x" section on page 29-7)
- Use Last (Rather than First) Redirecting Number for Routing Incoming Call
- Cross-Server settings

# Custom Keypad Mapping Tool in Cisco Unity Connection 10.x

The Custom Keypad Mapping tool allows you to edit the key mappings that are associated with the Custom Keypad Mapping conversations. Within each of these conversations—which are assigned to individual users or user templates on the **Phone Menu** page in Cisco Unity Connection Administration—there are eight different menus that can be customized. Changing key mappings by using this tool does not affect any of the other Cisco Unity Connection conversation versions.

You can assign any one-, two-, or three-key sequence to any defined option for the **Main** menu, the **Message Playback** menu (the message header, body and footer can be mapped separately), the **After Message** menu, the **Settings** menu, the **Message Settings** menu, and the **Preferences** menu. You can customize which options are voiced in each menu and the order in which they are offered.

See the following sections for details:


- Using the Custom Keypad Mapping Tool in Cisco Unity Connection 10.x, page 17-1
- Conversation Menus That Can Be Customized in Cisco Unity Connection 10.x, page 17-3
- Documenting Your Keymap in Cisco Unity Connection 10.x, page 17-13


## Using the Custom Keypad Mapping Tool in Cisco Unity Connection 10.x

The Custom Keypad Mapping tool is divided into eight tabs that represent eight different conversation menus that can be customized. On each of these menu tabs you can:

- Customize which key or keys are assigned to each menu option. Leaving a key assignment blank disables that option for the menu.
- Configure whether the option is voiced in the menu. This allows you to assign a key or keys to an option but not have it presented verbally in the menu. The option would still be enabled for that menu and Unity Connection would respond appropriately if the assigned key is pressed, but the user would not hear the option in the menu.
- Configure the order in which the menu items are offered to users. This is done by selecting the radio button of the row that you want to reorder and then using either the **Up** or **Down** arrows or the **Move To** button to arrange the menu items. The order in which the options appear in the tool is the order in which they are presented to the user by phone regardless of which keys are mapped to the options

### To Use the Custom Keypad Mapping Tool to Make Changes to a Custom Keypad Map

**Step 1** In Cisco Unity Connection Administration, expand **Tools**, then select **Custom Keypad Mapping**.

**Step 2** On the **Search Custom Keypad Mappings** page, select the applicable custom keypad mapping conversation.

**Note** Unity Connection supports 6 Custom Keypad Mappings.

**Step 3** On the **Edit Custom Keypad Mapping** page, select the applicable tab to select the menu for which you would like to change key assignments.

**Step 4** Change key assignments as applicable. (For guidelines on allowed entries, see the "Guidelines for Assigning Keys to Menu Options" section on page 17-2.)

**Step 5** Select **Save**.

When changes are saved, all new calls that use this conversation follow the new key mapping settings.

**Step 6** Repeat Step 3 through Step 5 for each menu that you want to customize.

# Guidelines for Assigning Keys to Menu Options

- The only characters allowed are: 0 – 9, *, # or blank.
- A maximum of 3 digits is allowed for each menu option.
- Duplicate key entries are not allowed for any unique menu. (For example, you cannot map the "1" key to both Hear New Messages and Send a Message in the Main menu. However, you can map the "1" key to Hear New Messages in the Main menu and also to Greetings in the Settings menu.)
- Leaving a key assignment blank disables that option for the menu.
- When you leave a key assignment black, uncheck the Option Voiced in Menu check box.
- When changes are saved, all new calls that use the conversation follow the new key mapping settings.

# Setting a Keypad Mapping to Match an Existing Conversation Mapping

You can change the key mappings for all menus to match that of an existing conversation. For example, you can have all of the key mappings for a selected custom keypad mapping replaced with the mappings of Optional Conversation 1. This can be useful if you want to make a small number of changes to an existing conversation and do not want to manually remap every option.

### To Set Key Mappings to an Existing Conversation

**Step 1** In Cisco Unity Connection Administration, expand **Tools**, then select **Custom Keypad Mapping**.

**Step 2** On the **Search Custom Keypad Mappings** page, select the applicable custom keypad mapping conversation.

**Step 3** On any tab of the **Edit Custom Keypad Mapping** page, in the **Reset Mappings on All Tabs To** list, select the conversation that you want to use and select **Reset**.

**Step 4** When asked to confirm that you want to replace all key mappings with those of the selected conversation before continuing, select **OK**.

# Conversation Menus That Can Be Customized in Cisco Unity Connection 10.x

The Custom Keypad Mapping tool is divided into eight tabs that represent eight different conversation menus that can be customized. The **Message Playback** menu is represented on three tabs because messages contain three distinct parts: the message header, the message body, and the message footer. The options on these three tabs are identical, but you may want to map different options to different keys for certain parts.

The following menus can be customized:

- Main Menu Tab, page 17-3
- Message Playback Menu Tabs (Message Header Tab, Message Body Tab, and Message Footer Tab), page 17-5
- After Message Menu Tab, page 17-9
- Settings Menu Tab, page 17-11
- Message Settings Menu Tab, page 17-12
- Preferences Menu Tab, page 17-12

## Main Menu Tab

The **Main** menu is what users hear immediately after they sign in and hear their message counts (if applicable).

See Table 17-1 for a list of options that can be mapped.

*Table 17-1 Main Menu Tab*

| Option | Description |
|---|---|
| Play New Messages | Takes users to the new (unread) message stack. |
| Send a Message | Takes users to the **Send Message** menu. |
| Review Old Messages | Takes users to the saved message stack. If applicable, users are also offered an opportunity to review deleted messages. |
| Change Setup Options | Takes users to the **Settings** menu where they can configure settings for greetings, transfer rules, and alternate contact numbers, and access their message settings and preferences. |
| Find Messages | Takes users to the **Message Locator** feature where they can search for new messages by the calling number or name of the sender.<br><br>This option is offered only when the **Finding Messages With Message Locator** feature is enabled for each user on the **Phone Menu** page. |

*Table 17-1 Main Menu Tab (continued)*

| Option | Description |
|---|---|
| List Meetings | Lists the time, meeting organizer, and subject for all current and upcoming meetings.<br>For Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express meetings, the user is offered the option to join current meetings.<br>**Note** Integrations with Cisco Unified MeetingPlace Express are not supported in Cisco Unity Connection. |
| Play External Messages | Provides the count of messages that are stored on an external message store.<br>The user is offered the option to listen to these messages. |
| Manage Call Handler Greetings | Allows users to access the Greetings Administrator conversation to change greetings for call handlers that have been assigned an extension.<br>Users who are assigned to the **Greetings Administrator** role on the **Edit Roles** page can change the greetings for any system call handler.<br>Users who are not assigned to the **Greetings Administrator** role can change the greetings only for call handlers that they own. |
| Call a Number | Allows users to access the User System Transfer conversation and dial any number that is allowed by their transfer restriction table. |
| Manage Broadcast Messages | Allows users to access the Broadcast Message Administration conversation.<br>This option is offered only when the **Send or Update Broadcast Messages** setting is configured for each user on the **Send Message Settings** page. |
| Repeat Menu Options | Plays the **Main** menu again. |
| Help | Plays the **Main** menu **Help**. |
| Cancel or Back Up | Exits the user mailbox.<br>By default, when users exit their mailboxes they are sent to the Opening Greeting call handler. However, you can customize the exit behavior by changing the When Exiting the Conversation setting on the Phone Menu page for each user. |

*Table 17-1 Main Menu Tab (continued)*

| Option | Description |
|---|---|
| Switch Between Using the Phone Keypad and Using Voice Commands | Allows users to toggle between the touchtone and voice-recognition conversations:<br>• When users are listening to the touchtone conversation, and press the applicable keys, they are immediately switched to the voice-recognition conversation.<br>• When users are listening to the voice-recognition conversation, and press the applicable keys, they are immediately switched to the touchtone conversation.<br>Note that the toggle persists until the user toggles back, or until the end of the call.<br>**Note** In case of a video call, the toggle key is not supported as Unity Connection 10.0(1) always plays touchtone conversation. |
| Change Alternate Greeting | Allows users to change alternate greetings by activating and re-recording.<br>In case of a video call, when users are listening to the main menu options and press the applicable key, Cisco Unity Connection will play your alternate video greeting and will ask you to re-record your alternate greeting. For more details on enabling alternate greetings for each user, see Allowing Users to Playback Video Greetings in Cisco Unity Connection 10.x, page 16-14. |

# Message Playback Menu Tabs (Message Header Tab, Message Body Tab, and Message Footer Tab)

When a message is played in the Cisco Unity Connection user conversation, there are three separate parts: the header, the body, and the footer. By default, the message header contains the message number and the sender information. The message body is the actual recording of the message. The message footer is the time stamp.

The contents of the header and footer sections can be modified on the **Playback Message Settings** page. For example, the message number, the sender information, the sender extension, and the time stamp can be added or removed from the header. These settings are controlled by the check boxes under the “Before Playing Each Message, Play” section on the **Playback Message Settings** page. For the message footer, you have the option of playing the time stamp after the message; you can exclude it altogether or have it played as part of the header. This option is controlled with the check box under the “After Playing Each Message, Play” section on the **Playback Message Settings** page. If you choose not to play the time stamp after the message, the effect is to have no footer to the message. In Cisco Unity Connection, the “After Playing Each Message, Play” section now includes the sender information, extension or ANI, and the message number, in addition to the time the message was sent and message duration.

The Custom Keypad Mapping tool includes separate tabs for each part of the message. As a best practice, we recommend that you map the same keys to each option for all three parts. However, in some cases it may be useful to map the same key to different actions. For example, during the message header you might want to press the “1” key to skip to the start of the message body, and during the message body press the “1” key to skip to the message footer.

The same message playback key mappings are used when listening to new messages, saved messages, and deleted messages, rather than separate mappings for each message stack. Keep this in mind as you are deciding on key mapping preferences, particularly for options such as marking messages as new (unread) or saved (read).

Message playback options are not voiced in a menu format by phone, but they are listed if the user presses the key that is mapped to the **Help** option. The Custom Keypad Mapping tool allows you to configure which items are voiced in the **Help**.

See Table 17-2 for a list of options that can be mapped.

***Table 17-2 Message Playback Menu Tabs***

| Option | Description |
|---|---|
| Repeat Message | Jumps to the beginning of the header portion of the message. |
| Save | Skips to the next message and marks the current message as saved. |
| Delete | Deletes the message that is currently being played.<br>The user class of service determines whether the message is moved to the deleted items folder or is deleted permanently. |
| Slow Playback | Slows down the message that is currently being played. Pressing the mapped key slows the message playback by 50 percent.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback speed is saved as the default playback speed for the user. |
| Fast Playback | Speeds up the message that is currently being played. Pressing the mapped key speeds the message playback by 50 percent. Pressing the key again speeds the message playback by 100 percent.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback speed is saved as the default playback speed for the user. |
| Reset Speed to Default | Resets the speed of the message that is currently being played to the default message playback speed setting for the user.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback speed is saved as the default playback speed for the user. |
| Change Volume | Cycles the volume of the message that is currently being played through three volume levels: normal, loud, and quiet.If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback volume is saved as the default playback volume for the user. |

*Table 17-2 Message Playback Menu Tabs (continued)*

| Option | Description |
|---|---|
| Reset Volume to Default | Resets the volume of the message that is currently being played to the default message playback volume setting for the user.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback volume is saved as the default playback volume for the user. |
| Quieter Playback | Decreases the volume of the message that is currently being played.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback volume is saved as the default playback volume for the user. |
| Louder Playback | Increases the volume of the message that is currently being played.<br>**Note** If the **Save Speed and Volume Changes Made by User** setting is enabled on the **System Settings > Advanced > Conversation Configuration** page, the last change made to playback volume is saved as the default playback volume for the user. |
| Pause/Resume | Pauses playback of the message, or resumes playback when the message is already paused. |
| Rewind | Jumps backward in the message that is currently being played.<br>By default, the message rewinds five seconds. You can adjust the rewind time on the **Playback Message Settings** page. |
| Fast-Forward | Jumps forward in the message that is currently being played.<br>By default, the message fast-forwards five seconds. You can adjust the fast-forward time on the **Playback Message Settings** page. |
| Skip to After Message Menu | Jumps directly to the **After Message** menu. |
| Skip Message, Save As Is | Skips to the next message in the stack and leaves the message in the state it was in. When a new message is skipped, it is saved as unread; when a saved message is skipped, it remains saved; and when a deleted message is skipped, it remains deleted. |
| Save as New | Skips to the next message in the stack and marks the message as new. When this option is selected, if a user skips messages when listening to saved or deleted messages, the messages are marked as unread and are moved to the new message stack. |
| Play Message By Number | Asks the user to enter the number of a message in the current stack (new, saved, or deleted messages) and then takes the user directly to that message. For users who have large numbers of messages, this is a useful way to jump ahead or back in the stacks.<br>This option is offered only when the **Enable Go to Message** setting is enabled on the **System Settings > Advanced > Conversation** page. |
| Go to Previous Message | Takes the user to the previous message in the stack. |

*Table 17-2 Message Playback Menu Tabs (continued)*

| Option | Description |
|---|---|
| Go to Next Message | Takes the user to the next message in the stack. The message the user was listening to is left in the state it was in (new, saved, or deleted). **Go to Next Message** functions the same as the **Skip Message**, **Save As Is** option. |
| Cancel or Back Up | Terminates message playback and goes up a menu level. Users who are listening to new or saved messages go to the **Main** menu. Users who are listening to deleted messages go to the **Deleted Message Option** menu. |
| Reply | Replies to the sender of the message. Only the sender receives the reply. Other recipients of the original message do not receive the reply.<br>This option is available only when the message is from another user; users cannot reply to outside caller messages. |
| Reply to All | Replies to all recipients of the message. |
| Call the Sender | Terminates message playback, signs users out of their mailboxes, and transfers users to the person who left the message. This feature is also known as **Live Reply.** This key option is used to return calls to both users and unidentified callers.<br>This option is available only when the user is assigned to a class of service that has enabled either the **Users Can Reply to Messages from Other Users by Calling Them** or the **Users Can Reply to Messages from Unidentified Callers by Calling Them** setting. |
| Forward Message | Allows the user to forward the message to another user or distribution list. |
| Forward Original Message | Forwards the original voice message and removes any forwarded introductions that may have been added to the message by previous forwards. |
| Skip to End | Jumps to the beginning of the message footer.<br>When the **After Playing Each Message**, Play options are not enabled for the user on the **Playback Message Settings** page, these options effectively skips to the end of the message and goes directly to the **After Message** menu. |
| Replay Message | Jumps to the beginning of the message body, effectively repeating the message. If you assign a key to this option for the message header, it allows users to skip the header and jump right to the message. |
| Play Message Properties | Plays the properties of the message that is currently being played. This includes the sender information (including ANI if it is provided for outside callers) and the time that the message was sent. |
| Operator | Signs users out of their mailboxes and sends them to the Operator call handler. The message is left in the state that it was in. |
| Go to First Message | Jumps to the first message of the message stack. Unity Connection plays the “First message” prompt as an audible cue to the user. |
| Go to Last Message | Jumps to the last message of the message stack. Unity Connection plays the “Last message” prompt as an audible cue to the user. |
| List Message Recipients | Lists all recipients of the current message. |

*Table 17-2 Message Playback Menu Tabs (continued)*

| Option | Description |
|---|---|
| Toggle Urgency Flag | Toggles the priority flag on a received message between urgent and normal.<br>Users who want to identify the high-priority messages among all of their received messages may be interested in this functionality. By default, Unity Connection plays messages that are marked urgent first. |
| Send to Fax Machine for Printing | Sends the message to a fax machine. This option is available for fax messages and any message that has an attachment that can be sent to a fax machine.<br>This option is available only when fax is configured as an external service for the user. |
| Help | Plays **Help** for all of the options that are mapped to a key, and for which the **Option Voiced in Help** check box is checked. |
| Play Message Attachments | Describes the files that are attached to the message. Files in compatible formats are played or read. |

# After Message Menu Tab

The **After Message** menu plays after the user has listened to a message.

See Table 17-3 for a list of options that can be mapped.

*Table 17-3 After Message Menu Tab*

| Option | Description |
|---|---|
| Repeat Message | Plays the message again, starting with the header. |
| Save | Marks the message as saved (read) and moves to the next message in the stack. When the user is listening to a deleted message, this option moves the message to the saved message stack. |
| Delete | Deletes the message that is currently being played.<br>The user class of service determines whether the message is moved to the deleted items folder or is deleted permanently. |
| Reply | Replies to the sender of the message. Only the sender receives the reply; other recipients of the original message do not receive the reply.<br>This option is available only when the message is from another user; users cannot reply to outside caller messages. |
| Forward Message | Allows the user to forward the message to another user or distribution list. |
| Forward Original Message | Forwards the original voice message and removes any forwarded introductions that may have been added to the message by previous forwards. |
| Save as New | Marks the message as new (unread) and moves to the next message in the stack. When the user is listening to a saved or deleted message, this option moves the message to the new message stack. |

*Table 17-3 After Message Menu Tab (continued)*

| Option | Description |
|---|---|
| Rewind | Jumps backward into the message.<br>By default, the message rewinds five seconds. You can adjust the rewind time on the Playback Message Settings page. |
| Send to Fax Machine for Printing | Sends the message to a fax machine. This option is available for fax messages and any message that has an attachment that can be sent to a fax machine.<br>This option is available only when fax is configured as an external service for the user. |
| Play Message Properties | Plays the properties of the current message. This includes the sender information (including ANI if it is provided for outside callers) and the time that the message was sent. |
| Cancel or Back Up | Exits the **After Message** menu and goes up a menu level. Users who are listening to new or saved messages go to the **Main** menu. Users who are listening to deleted messages go to the **Deleted Message Option** menu. |
| Help | Plays the After Message menu Help. |
| Operator | Signs users out of their mailboxes and sends them to the operator call handler. The message is left in the state it was in. |
| Play Message Attachments | Describes the files that are attached to the message. Files in compatible formats are played or read. |
| Play Message By Number | Asks the user to enter the number of a message in the current stack (new, saved, or deleted messages) and then takes the user directly to that message. For users who have large numbers of messages, this is a useful way to jump ahead or back in the stacks.<br>This option is available only when the **Enable Go to Message** setting is enabled on the **System Settings > Advanced > Conversations** page. |
| Go to Previous Message | Takes the user to the previous message in the stack. |
| Go to Next Message | Takes the user to the next message in the stack. The message the user was listening to is left in the state that it was in (new, saved, or deleted). **Go to Next Message** functions the same as the **Skip Message**, **Save As Is** option. |
| Save As Is | Goes to the next message in the stack and leaves the message in the state that it was in. New messages are saved as unread; saved messages remain saved; and deleted messages remain deleted. |
| Go to First Message | Jumps to the first message of the message stack. Unity Connection plays the “First message” prompt as an audible cue to the user. |
| Go to Last Message | Jumps to the last message of the message stack. Unity Connection plays the “Last message” prompt as an audible cue to the user. |
| Toggle Urgency Flag | Toggles the priority flag on a received message between urgent and normal.<br>Users who want to identify the high-priority messages among all of their received messages may be interested in this functionality. By default, Unity Connection plays messages that are marked urgent first. |

*Table 17-3 After Message Menu Tab (continued)*

| Option | Description |
|---|---|
| Call the Sender | Terminates message playback, signs users out of their mailboxes, and transfers users to the person who left the message. This feature is also known as **Live Reply**. This key option is used to return calls to both other users and unidentified callers.<br><br>This option is available only when the user is assigned to a class of service that has enabled either the **Users Can Reply to Messages from Other Users by Calling Them** or the **Users Can Reply to Messages from Unidentified Callers by Calling Them** setting. |
| Skip Message, Save As Is | Skips to the next message in the stack and leaves the message in the state it was in. When a new message is skipped, it is saved as unread; when a saved message is skipped, it remains saved; and when a deleted message is skipped, it remains deleted. |
| List Message Recipients | Lists all recipients of the current message. |
| Reply to All | Replies to all recipients of the message. |

# Settings Menu Tab

The Settings menu is what users hear when they choose **Change Setup Options** from the **Main** menu.

See Table 17-4 for a list of options that can be mapped.

*Table 17-4 Settings Menu Tab*

| Option | Description |
|---|---|
| Greetings | Allows users to modify their greetings. |
| Message Settings | Takes users to the Message Settings menu. |
| Preferences | Takes users to the Preferences menu. |
| Transfer Settings | Allows users to modify their transfer rules. |
| Alternate Contact Numbers | Allows users to change their alternate contact phone numbers.<br><br>This option is available for a user only when an administrator has configured one or more caller input keys to transfer to an alternate contact number on the user **Edit Caller Input** page. |
| Repeat Menu | Plays the **Settings** menu again. |
| Help | Plays the **Settings** menu **Help**. |
| Cancel or Back Up | Exits the **Settings** menu and goes up a menu level to the **Main** menu. |
| Change Alternate Greeting | Allows users to change alternate greetings by activating and re-recording.<br><br>In case of a video call, when users are listening to the main menu options and press the applicable key, Cisco Unity Connection will play your alternate video greeting and will ask you to re-record your alternate greeting. For more details on enabling alternate greetings for each user, see Allowing Users to Playback Video Greetings in Cisco Unity Connection 10.x, page 16-14. |

# Message Settings Menu Tab

The Message Settings menu is what users hear when they choose Message Settings from the Settings menu.

See Table 17-5 for a list of options that can be mapped.

*Table 17-5 Message Settings Menu Tab*

| Option | Description |
|---|---|
| Message Notification | Allows users to modify the settings for their message notification devices. |
| Fax Delivery | Allows users to change the phone number of the fax machine to which they can send faxes for printing. |
| Menu Style | Allows users to switch between the full or brief menu styles. |
| Private Lists | Allows users to modify their private lists. |
| Addressing Priority List | Allows users to review and add or remove names from their addressing priority list. |
| Repeat Menu | Plays the Message Settings menu again. |
| Help | Plays the Message Settings menu Help. |
| Cancel or Back Up | Exits the Message Settings menu and goes up a menu level to the Settings menu. |

# Preferences Menu Tab

The **Preferences** menu is what users hear when they choose **Preferences** from the **Settings** menu.

See Table 17-6 for a list of options that can be mapped.

*Table 17-6 Preferences Menu Tab*

| Option | Description |
|---|---|
| Change Phone Password | Allows users to modify their phone PINs.<br>This option is not available for a user when the **User Cannot Change** check box is checked on the user **Edit Password Settings** page. |
| Change Recorded Name | Allows users to record names.<br>This option is available only when the user is assigned to a class of service that has enabled the **Allow Recording of Name** option. |
| Change Directory Listing | Allows users to choose whether or not they want to be listed in the directory.<br>This option is available only when the user is assigned to a class of service that has enabled the **Allow Users to Choose to Be Listed in the Directory** option. |
| Edit User-Defined Alternate Extensions | Allows users to list and delete their alternate extensions. Also allows users to add the current number they are calling from as an alternate extension (if it is not already an alternate extension and does not match a blocked pattern in the **User-Defined or Automatically-Added Alternate Extensions** restriction table). |

*Table 17-6 Preferences Menu Tab (continued)*

| Option | Description |
|---|---|
| Repeat Menu | Plays the **Preferences** menu again. |
| Help | Plays the **Preferences** menu **Help**. |
| Cancel or Back Up | Exits the **Preferences** menu and goes up a menu level to the **Settings** menu. |

# Documenting Your Keymap in Cisco Unity Connection 10.x

The Wallet Card wizard is available for producing a PDF file of a wallet card based on your custom keypad mappings. For details, see the "Wallet Card Wizard in Cisco Unity Connection 10.x" section on page 3-10.

# Changing the Audio Format of Recordings and Media Streams in Cisco Unity Connection 10.x

See the following sections:


- Changing the Audio Format That Cisco Unity Connection 10.x Uses for Calls, page 18-1
- Changing the Audio Format for Recordings in Cisco Unity Connection 10.x, page 18-2


## Changing the Audio Format That Cisco Unity Connection 10.x Uses for Calls

For calls, Cisco Unity Connection advertises the audio format (or codec) that is preferred for the media stream with the phone system. You should consider the following when setting the audio format:

- When Unity Connection advertises a different audio format than the one used by the phone system, the phone system transcodes the media stream.
- Unity Connection should use the same audio format for the media stream that the phone system uses for the following reasons:
  - To reduce the need for transcoding the media stream from one audio format to another.
  - To minimize the performance impact on the Unity Connection server and on the phone system.
  - To preserve the audio quality of calls.

For more information on audio format codecs, see the "Audio Codecs" section in the "Sizing and Scaling Cisco Unity Connection 10.x Servers" chapter of the *Design Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html.

### To Change the Audio Format That Cisco Unity Connection Uses for Calls

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

**Step 2** On the **Search Port Groups** page, select the port group that belongs to the phone system integration for which you want to change the audio format of the media stream.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Codec Advertising**.

**Step 4** On the **Edit Codec Advertising** page, select the **Up** and **Down** arrows to change the order of the codecs or to move codecs between the **Advertised Codec** box and the **Unadvertised Codecs** box.

If only one codec is in the **Advertised Codecs** box, Cisco Unity Connection sends the media stream in that audio format. The phone system transcodes if it does not use this audio format.

If two or more codecs are in the **Advertised Codecs** box, Unity Connection advertises its preference for the first codec in the list but sends the media stream in the audio format from the list that the phone system selects.

**Step 5** Select **Save**.

**Step 6** *(All integrations except SCCP)* If you want to change the packet size that is used by the advertised codecs, on the **Port Group Basics** page, under **Advertised Codec** Settings, select the applicable packet setting for each codec in the Packet Size list, and select **Save**.

**Step 7** On the **Port Group** menu, select **Search Port Groups**.

**Step 8** Repeat Step 2 through Step 7 for all remaining port groups that belong to the phone system integration for which you want to change the audio format of the media stream.

# Changing the Audio Format for Recordings in Cisco Unity Connection 10.x

Typically, you configure Cisco Unity Connection to use the same audio format (or codec) for recording a message that the playback device uses. For example, if users listen to messages primarily on a phone system extension, you should configure Unity Connection to record messages in the same audio format that the phone system uses. If users listen to messages on Personal Digital Assistants (PDAs), however, you should configure Unity Connection to record messages in the audio format that the PDAs use (such as GSM 6.10).

Consider the following when setting the audio format for recording messages:

- Setting the audio format for recordings affects all messages, greetings, and names systemwide for all users.
- The audio format that you choose affects only recordings made by phone, either by using the TUI or by using the Media Master and TRAP. Recordings made by using the Media Master and a microphone are always stored in G.711 mu-law.
- Minimizing the number of different audio formats in use by Unity Connection for recording and playing recorded messages, greetings, and names reduces transcoding between audio formats that Unity Connection must perform, and thus reduces the effect on the performance of the Unity Connection server.
- When a message, greeting, or name is recorded in a lower quality audio format and later transcoded to a higher quality audio format during playback, the sound quality is not improved. Usually, the sound quality of a recording suffers during transcoding, especially when the sampling rate is changed.

  For example, sound quality suffers when messages that are recorded in the G.729a audio format are played on devices that use the G.711 Mu-Law audio format. However, sound quality is preserved when messages that are recorded in the G.711 Mu-Law audio format are played on devices that use the same audio format.
- Changing the audio format for recordings affects only messages, greetings, and names that are recorded after the setting is changed. Existing messages, greetings, and names that were recorded in a different audio format are not affected by the new setting.

For more information on audio format codecs, see the "Audio Codecs" section in the "Sizing and Scaling Cisco Unity Connection 10.x Servers" chapter of the *Design Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html.

### To Change the Audio Format for Recording Messages By Using the Phone

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **Edit General Configuration** page, in the **Recording Format** list, select the applicable setting.

**Note** If the playback device uses a different audio format, Unity Connection must transcode the messages, greetings, and names into the applicable audio format or the playback device is not able to play them.

**Step 3** Select **Save**.

# Changing the Video Format of Greetings in Cisco Unity Connection 10.x

See the following sections:


- Changing the Video Format that Cisco Unity Connection 10.x Uses for Calls, page 19-1
- Changing the Video Format for Greetings in Cisco Unity Connection 10.x, page 19-2


## Changing the Video Format that Cisco Unity Connection 10.x Uses for Calls

For calls, Cisco Unity Connection advertises the video format (or codec) that is preferred for the media stream with the phone system. You should consider the following when setting the video format:

- When Unity Connection advertises a different video format than the one used by the phone system, the phone system transcodes the media stream.
- Unity Connection should use the same video format for the media stream that the phone system uses for the following reasons:
  - To reduce the need for transcoding the media stream from one video format to another.
  - To minimize the performance impact on the Unity Connection server and on the phone system.
  - To preserve the video quality of calls.

**Note** In Cisco Unity Connection 10.0(1), only G.711 μ-law codec is supported for audio and H.264 codec is supported for video.

For more information on video format codecs, see the "Video Codecs" section in the "Sizing and Scaling Cisco Unity Connection 10.x Servers" chapter of the *Design Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html.

### To Change the video Format That Cisco Unity Connection Uses for Calls

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

**Step 2** On the **Search Port Groups** page, select the port group that belongs to the phone system integration for which you want to change the video format of the media stream.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Codec Advertising**.

**Step 4** On the **Edit Codec Advertising** page, select the **Up** and **Down** arrows to change the order of the codecs or to move codecs between the **Advertised Codec** box and the **Unadvertised Codecs** box.

If only one codec is in the **Advertised Codecs** box, Cisco Unity Connection sends the media stream in that audio format. The phone system transcodes if it does not use this audio format.

If two or more codecs are in the **Advertised Codecs** box, Unity Connection advertises its preference for the first codec in the list but sends the media stream in the audio format from the list that the phone system selects.

**Step 5** Select **Save**.

**Step 6** *(Only SIP integrations)* If you want to change the packet size that is used by the advertised codecs, on the **Port Group Basics** page, under **Advertised Codec Settings**, select the applicable packet setting for each codec in the **Packet Size** list, and select **Save**.

**Note** For both the audio and video calls, change the packet size for the codecs G711, G729, and G722 in Cisco Unified Communications Manager and the remaining codecs will be changed in Cisco Unity Connection Administration.

**Step 7** On the **Port Group** menu, select **Search Port Groups**.

**Step 8** Repeat Step 2 through Step 7 for all remaining port groups that belong to the phone system integration for which you want to change the video format of the media stream.

# Changing the Video Format for Greetings in Cisco Unity Connection 10.x

Typically, you configure Cisco Unity Connection to use the same video format (or codec) for recording a video greeting that the playback device uses. For example, if users listen to greetings primarily on a phone system extension, you should configure Unity Connection to record video greetings in the same video format that the phone system uses. If users listen to video greetings on Personal Digital Assistants (PDAs), however, you should configure Unity Connection to record greetings in the video format that the PDAs use (such as GSM 6.10).

Consider the following when setting the video format for recording messages:

- Setting the video format for recordings affects all video greetings systemwide for all users.
- Minimizing the number of different video formats in use by Unity Connection for recording and playing video greetings reduces transcoding between video formats that Unity Connection must perform, and thus reduces the effect on the performance of the Unity Connection server.
- When a video greeting is recorded in a lower quality video format and later transcoded to a higher quality video format during playback, the sound quality is not improved. Usually, the sound quality of a greeting suffers during transcoding, especially when the sampling rate is changed.

  For example, sound quality suffers when messages that are recorded in the G.729a video format are played on devices that use the G.711 µ-Law video format. However, sound quality is preserved when messages that are recorded in the G.711 µ-Law video format are played on devices that use the same video format.

For more information on video format codecs, see the "video Codecs" section in the ""Sizing and Scaling Cisco Unity Connection 10.x Servers" chapter of the *Design Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html.

### To Change the video Format for Greetings By Using the Phone

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **Edit General Configuration** page, in the **Recording Format** list, select the applicable setting.

**Note** If the playback device uses a different video format, Unity Connection must transcode the messages, greetings, and names into the applicable video format or the playback device is not able to play them.

**Step 3** Select **Save**.

# Managing Recorded Greetings and Recorded Names in Cisco Unity Connection 10.x

You can record names for users, system distribution lists, and call handlers (including interview handlers and directory handlers), and greetings for users and call handlers, by using the Media Master on the pages within Cisco Unity Connection Administration. In circumstances when you cannot access Connection Administration, you can access the Cisco Unity Greetings Administrator from any phone to manage greetings for call handlers.

Note that users can record their own names and personal greetings by accessing the Cisco Unity Connection conversation by phone, or by using the Media Master in the Unity Connection Messaging Assistant web tool. For end-user instructions and information about using the Media Master, see the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html.

See the following sections for details:


- Using the Media Master to Record Greetings and Names in Cisco Unity Connection 10.x, page 20-1
- Using the 10.x Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings, page 20-2
- Setting Up the 10.x Cisco Unity Greetings Administrator, page 20-4
- Changing the Audio Format for Recording Greetings and Names in Cisco Unity Connection 10.x, page 20-5


## Using the Media Master to Record Greetings and Names in Cisco Unity Connection 10.x

The Media Master appears on each page of Cisco Unity Connection Administration on which recordings can be made. It allows you to make and play recordings, either with a phone or with your computer microphone and speakers, by selecting the Media Master controls. In addition, the Options menu on the Media Master allows you to use other sound (WAV) files in your recordings.

When determining the recording and playback device that you want to use with the Media Master in Connection Administration, consider the following points:

- The phone serves as the default recording and playback device for the Media Master.

- The phone offers the best sound quality for recordings.

  In order to use the phone as a recording and playback device, Unity Connection must have at least one voice messaging port designated to allow users to use the phone as a recording and playback device. Alternatively, when you make and play recordings by using a computer microphone and speakers, no ports are used, which decreases the load on the Unity Connection server and leaves ports open for other functions.

Use the following procedure to select the recording and playback device used by the Media Master. Updates to the Media Master are saved per user, per computer. If you plan to use additional computers to access Cisco Unity Connection Administration, the Media Master needs to be set up on each.

**To Select a Recording and Playback Device**

**Step 1** In Cisco Unity Connection Administration, go to a page on which the Media Master appears.

**Step 2** On the **Media Master Options** menu, select **Playback & Recording**.

**Step 3** In the **Playback & Recording Settings** dialog box, select a playback device and a recording device.

**Step 4** If you chose the phone as the recording and playback device in Step 3, the **Active Phone Number** is set by default to your primary extension. To specify a different phone number, enter it in the **Other Number** field.

**Note** After changing the timeout value in telephone record and playback (TRAP), you need to restart the **Conversation Manager** and **Tomcat** services to reflect the changes.

**Step 5** Select **OK**.

# Using the 10.x Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings

The Cisco Unity Greetings Administrator allows you—or the call handler owners that you assign—to manage call handler greetings from any phone. The owner of the call handler can be any user

By using the Cisco Unity Greetings Administrator, you can do the following tasks without having to access the Media Master in Cisco Unity Connection Administration:

- Rerecord a call handler greeting.
- Toggle between the alternate and standard greetings.
- Determine which greeting is currently active for a call handler.
- Listen to and record busy, closed, internal, and holiday greetings.

For example, if your office is unexpectedly closed because of bad weather, you can call Unity Connection from home to enable the alternate Opening Greeting, or rerecord a call handler greeting to state that the office is closed.

With a multilingual system, if the call handler greetings language is inherited, you have the option of providing call handler greetings in multiple languages. For example, if Cisco Unity Connection is set up to provide prompts in French and Spanish, you might record the call handler greeting in both languages so that Spanish- and French-speaking callers can hear your greeting in their own language.

If you do not record a greeting in a language your system provides, Unity Connection plays the system default greeting for calls that are associated with that greeting. For example, if you recorded the standard greeting in French, but not in Spanish, Spanish-speaking callers would hear the system default greeting for the call handler while French-speaking callers would hear the French greeting you recorded.

To access the Cisco Unity Greetings Administrator, the owner of the call handler requires the following information:

- The phone number to dial for access to the Cisco Unity Greetings Administrator

  Alternatively, if you set up one-key dialing access to the Cisco Unity Greetings Administrator from the Opening Greeting, the owner of the call handler needs to know which key to press while listening to the Opening Greeting.
- The ID of the call handler owner
- The password of the call handler owner
- The extension of the call handler

To prevent unauthorized access to Unity Connection, make sure that the call handler owner understands that the above information should be kept confidential.

### To Use the Cisco Unity Greetings Administrator to Manage Call Handler Greetings

**Step 1** On the phone, dial the phone number for access to the Cisco Unity Greetings Administrator.

**Step 2** At the prompt, enter the ID of the call handler owner, and press **#**.

**Step 3** At the prompt, enter the password of the call handler owner, and press **#**.

**Step 4** At the prompt, enter the extension of the call handler, and press **#**.

**Step 5** If the call handler you selected in Step 4 is configured to inherit the caller language and there is more than one language installed on your Unity Connection system, at the prompt, press the number of the language in which to edit greetings for the call handler. (Unity Connection plays the **Greetings** menu options in the same language.)

**Step 6** Follow the Cisco Unity Greetings Administrator conversation to toggle between the alternate and standard call handler greetings, or to record the call handler greeting.

| | |
|---|---|
| **To toggle between standard and alternate greetings** | Press 1. |
| **To change the standard greeting** | Press 2. |
| **To change the alternate greeting** | Press 6. |

**Step 7** You can also use the Cisco Unity Greetings Administrator to record or listen to additional greetings.

| | |
|---|---|
| **To change the busy greeting** | Press 3. |
| **To change the closed greeting** | Press 4. |
| **To change the internal greeting** | Press 5. |
| **To change the holiday greeting** | Press 7. |

# Setting Up the 10.x Cisco Unity Greetings Administrator

To set up the Cisco Unity Greetings Administrator, do the following tasks:

1. Set up a phone number so that you or another user can call the Cisco Unity Greetings Administrator. For information on how to set up the phone number, see the documentation for your phone system.

   Alternatively, you can set a one-key dialing option from the Opening Greeting that takes callers to the Cisco Unity Greetings Administrator. Do the "To Set Up a One-Key Dialing Option From the Opening Greeting for Accessing the Cisco Unity Greetings Administrator" procedure on page 20-4. (If you choose this option, skip Task 2.)
2. If applicable, add a routing rule to forward calls to the Cisco Unity Greetings Administrator from the phone number that you set up in Task 1. Do the "To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator" procedure on page 20-4.
3. Assign a unique extension to each call handler that you want to access by using the Cisco Unity Greetings Administrator. Do the "To Assign a Unique Extension to a Call Handler" procedure on page 20-5.
4. As needed, tell call handler owners how to use the Cisco Unity Greetings Administrator. For an overview and procedure, see the "Using the 10.x Cisco Unity Greetings Administrator to Record or Rerecord Call Handler Greetings" section on page 20-2.

### To Set Up a One-Key Dialing Option From the Opening Greeting for Accessing the Cisco Unity Greetings Administrator

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handler** page, in the Search Results table, select the **Opening Greeting** call handler.

**Step 3** On the **Edit Call Handler Basics** page, on the **Edit** menu, select **Caller Input**.

**Step 4** On the **Caller Input** page, in the **Caller Input Keys** table, select the applicable phone keypad key.

**Step 5** On the **Edit Caller Input** page for the key that you selected, check the **Ignore Additional Input (Locked)** check box, if applicable.

Make sure that you did not select a phone keypad key in Step 4 that represents the first digit of the extensions on your phone system. If you lock that key, callers are not able to dial a user extension from the opening greeting.

**Step 6** Select **Conversation**, and then select **Greetings Administrator** in the list.

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

### To Add a Routing Rule to Forward Calls to the Cisco Unity Greetings Administrator

**Step 1** In Cisco Unity Connection Administration, expand **Call Management > Call Routing**, then select **Direct Routing Rules**.

**Step 2** On the **Direct Routing Rules** page, select **Add New**.

**Step 3** On the **New Direct Routing Rule** page, enter a display name for the new routing rule, and select **Save**.

**Step 4** On the **Edit Direct Routing Rule** page, confirm that the **Status** is set to **Active**.

**Step 5** In the **Routing Rule Conditions** table, select **Add New**.

**Step 6** On the **New Direct Routing Rule Condition** page, select **Dialed Number**, set a parameter in the list, and enter the phone number that has been set up for access to the Cisco Unity Greetings Administrator.

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

**Step 8** On the **Edit** menu, select **Edit Direct Routing Rule**.

**Step 9** On the **Edit Direct Routing Rule** page, in the **Send Call To** field, select **Conversation**, then select **Greetings Administrator**.

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

**Step 11** On the **Direct Routing Rule** menu, select **Direct Routing Rules**. Verify that the new routing rule is in an appropriate position with the other routing rules in the table. If you want to change the rule order, continue with Step 12.

**Step 12** Select **Change Order**.

**Step 13** On the **Edit Direct Routing Rule Order** page, select the name of the rule that you want to reorder, and select the **Up** or **Down** arrow until the rules appear in the correct order.

**Step 14** Select **Save**.

#### To Assign a Unique Extension to a Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, in the **System Call Handlers** table, select the display name of the call handler that you want to access with the Cisco Unity Greetings Administrator.

**Step 3** On the **Edit Call Handler Basics** page, in the **Extension** field, enter a unique extension for the call handler.

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

# Changing the Audio Format for Recording Greetings and Names in Cisco Unity Connection 10.x

Typically, Cisco Unity Connection uses the same audio format (or codec) for recording a greeting or name that the playback device uses. For example, if users listen to recorded greetings and recorded names on a phone system extension, Unity Connection should record greetings and names in the same audio format that the phone system uses.

You should consider the following when setting the audio format for recording greetings and names:

- Setting the audio format for recordings affects all messages, greetings, and names systemwide for all users.
- Minimizing the number of different audio formats in use for recording and playing recorded messages, greetings, and names reduces transcoding between audio formats that Unity Connection must perform, and reduces the effect on the performance of the Unity Connection server.

- When a message, greeting, or name is recorded in a lower quality audio format and later transcoded to a higher quality audio format during playback, the sound quality is not improved. Usually, the sound quality of a recording suffers during transcoding, especially when the sampling rate is changed.

  For example, sound quality suffers when greetings that are recorded in the G.729a audio format are played on devices that use the G.711 μ-Law audio format. However, sound quality is preserved when greetings that are recorded in the G.711 μ-Law audio format are played on devices that use the same audio format.
- Changing the audio format for recordings affects only messages, greetings, and names that are recorded after the setting is changed. Existing messages, greetings, and names that were recorded in a different audio format are not affected by the new setting.

### To Change the Audio Format for Recording Greetings and Names

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **Edit General Configuration** page, in the **Recording Format** list, select the applicable setting. Unity Connection records all messages, greetings, and names in the audio format that you select.

**Note** If the playback device uses a different audio format, Unity Connection must transcode the messages, greetings, and names into the applicable audio format or the playback device is not able to play them.

**Step 3** Select **Save**.

# Specifying Password, PIN, Sign-In, and Lockout Policies in Cisco Unity Connection 10.x

In Cisco Unity Connection10.x, you use authentication rules to determine the password, PIN, and account lockout policies for phone and web-tool access, and to specify the sign-in policy for web-tool access for all users who access Cisco Unity Connection voice messages.

See the following sections:


- Specifying Password, PIN, Sign-In, and Lockout Policies by Using Authentication Rules, page 21-1
- Creating and Modifying Authentication Rules, and Assigning Rules to Users, page 21-2


## Specifying Password, PIN, Sign-In, and Lockout Policies by Using Authentication Rules

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. You use authentication rules to secure how users access Unity Connection by phone, and how users access Cisco Unity Connection Administration and the Cisco Personal Communications Assistant (PCA).

For example, an authentication rule determines:

- The number of failed sign-in attempts that are allowed before an account is locked
- The number of minutes an account remains locked before it is reset
- Whether a locked account must be unlocked manually by an administrator
- The minimum length allowed for passwords and PINs
- The number of days before a password or PIN expires
- The number of days during which the expiry warning prompt (after which your credentials will expire) will be played.

**Note** The Administration can enable or disable the Cisco Unity Connection telephone user interface (touchtone conversation) PIN using the Command Line Interface (CLI). For more information on the CLI commands, see the **Utils Command** section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/10_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100.html.

# Creating and Modifying Authentication Rules, and Assigning Rules to Users

Authentication rules are specified on the **System Settings > Authentication Rules** page in Cisco Unity Connection Administration. Unity Connection includes the following predefined authentication rules:

| | |
|---|---|
| **Recommended Voicemail Authentication Rule** | By default, Unity Connection applies this rule to the voicemail PIN on the Password Settings page of each user account and user template for which you set up user access to Unity Connection by phone. |
| **Recommended Web Application Authentication Rule** | By default, Unity Connection applies this rule to the Web Application password on the Password Settings page of each user account and user template for which you set up user access to Cisco Unity Connection Administration, or to the Cisco Personal Communications Assistant. |

You can change these defaults, and can create an unlimited number of additional authentication rules.

For user accounts and templates, you specify the authentication rule that governs user access to Unity Connection. For information on specifying an authentication rule for a user account or template, see the "Passwords and PINs in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Messaging in Cisco Unity Connection 10.x

After you have implemented a call management plan and have determined conversation versions and options, you are ready to focus on how Cisco Unity Connection collects, handles, and stores messages. This chapter outlines the types of messages that are available in Unity Connection, and discusses how Unity Connection handles the recording, delivery, and storage of messages.

See the following sections:


- Types of Messages in Cisco Unity Connection 10.x, page 22-1
- Message Recording in Cisco Unity Connection 10.x, page 22-5
- Default Recipient Accounts in Cisco Unity Connection 10.x, page 22-7
- Dispatch Messages in Cisco Unity Connection 10.x, page 22-8
- Message Delivery in Cisco Unity Connection 10.x, page 22-10
- Message Delivery and Sensitivity Options in Cisco Unity Connection 10.x, page 22-14
- Message Actions in Cisco Unity Connection 10.x, page 22-16
- Message Subject Line Formats in Cisco Unity Connection 10.x, page 22-17
- Message Storage and Disk Capacity in Cisco Unity Connection 10.x, page 22-20
- Deleting Messages in Cisco Unity Connection 10.x, page 22-20
- Message Access in Cisco Unity Connection 10.x, page 22-22
- Configuring Live Record in Cisco Unity Connection 10.x, page 22-22
- Configuring Access to RSS Feeds of Voice Messages in Cisco Unity Connection 10.x, page 22-25


For information on securing user messages, see the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.

# Types of Messages in Cisco Unity Connection 10.x

Cisco Unity Connection supports a number of different types of messages that can be used depending on the needs of the organization.

### Unidentified (Outside Caller) Voice Messages

Callers who are not Cisco Unity Connection users—and those who have not signed in to Unity Connection—can reach user mailboxes to leave messages in a number of different ways, depending on the Unity Connection configuration. A caller can call the main phone number for the Unity Connection

server and spell by name or enter an extension to reach the user by using a directory handler, or can be directed to the user mailbox (or to a distribution list) through a call handler. Or, the caller can call the user extension and be forwarded to Unity Connection when the user does not answer, and then leave a message.

Unity Connection identifies the senders of these messages as unidentified callers. When an unidentified caller leaves a message, the From field of the message displays "UnityConnection@<servername>" in the Unity Connection Web Inbox or in an email client or an RSS reader, if applicable. Depending on whether the Subject line has been customized, it displays the phone number of the caller if it is available.

Messages from outside callers can be forwarded to other users, but cannot be replied to. However, depending on their class of service, users can "live reply" to a message from an unidentified caller by calling the sender after message playback.

#### User to User Voice Messages

Users can call Cisco Unity Connection and sign in, then send a message to one or more other Unity Connection users or to a distribution list. Unity Connection identifies the sender of the message as a user; when the called user later listens to the message, Unity Connection plays the recorded name of the user (or displays the username when the called user views the message in a Cisco web application such as the Unity Connection Web Inbox or from an IMAP client).

Alternatively, a user can call the extension of another user and be forwarded to Unity Connection when the called user does not answer, and then leave a message. In this case, if Identified User Messaging is enabled and supported by the phone system, and the user is calling from his or her primary extension or an alternate device, Unity Connection recognizes that the calling extension is associated with a user and identifies that user as the sender of the message.

**Note** Cisco Unity Connection does not perform any caller authentication or verification when a message is left by a caller who is identified as a user via Identified User Messaging.

Identified User Messaging is enabled by default. You can disable it for all users by using the Disable Identified User Messaging Systemwide setting on the System Settings > Advanced > Conversations page.

Users can reply to or forward messages from other users. Depending on their class of service, users can also "live reply" to a message from another user by calling the sender after message playback.

#### Email Messages in Exchange

Cisco Unity Connection can access email messages that are stored in user mailboxes in Microsoft Exchange and then the messages can be played by using text to speech (TTS).

#### System Broadcast Messages

System broadcast messages are recorded announcements that are sent to everyone in an organization. System broadcast messages are played immediately after users sign in to Cisco Unity Connection by phone—even before they hear message counts for new and saved messages. Users must listen to each system broadcast message in its entirety before Unity Connection allows them to hear new and saved messages or to change setup options. They cannot fast-forward or skip a system broadcast message.

**Note** By design, system broadcast messages do not trigger message waiting indicators (MWIs) on user phones. System broadcast messages also do not trigger message notifications for alternative devices, such as a pager or another phone.

See the "Setting Up Broadcast Messaging in Cisco Unity Connection 10.x" chapter for more information on setting up and using system broadcast messages.

### Text Notifications

Cisco Unity Connection can send message notifications in the form of text messages to email addresses, and also to text pagers and text-compatible mobile phones. When a message arrives that matches the criteria selected in the message notification settings, the Unity Connection Messaging System sends a text message entered by you or the user, such as "Urgent message for Technical Support." Unity Connection can also dial a phone number to alert the user of a new message and allow the user to enter credentials to sign in and listen to the message.

By default, if Unity Connection sends a notification of a new message to a device (such as a mobile phone) and the device forwards the call back to Unity Connection because the device did not answer, Unity Connection rejects the forwarded message notification call. As a result, the user mailbox is not filled with forwarded message notification announcements. Because Unity Connection rejects the forwarded message notification call, the call does not create a new message for the user and does not trigger a new message notification call.

See the "Notification Devices in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x* for more information on setting up various types of notifications. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

### HTML Notifications

Cisco Unity Connection allows you to deliver the SMTP-based HTML notifications for a new voice message to the end users. These notifications can be sent via SMTP as an HTML format embedded in the email. The users get the flexibility to receive the HTML notifications that can include customized icons, header, and footer along with the link to access Cisco Unity Connection Mini Web Inbox. Unity Connection Mini Web Inbox is a player that allows the user to play the notified messages over computer or mobile devices. The HTML notifications on the computer support both Web email clients (for example, Gmail) and desktop email clients (for example, Microsoft Outlook and IBM Lotus Notes). However, the HTML notifications on the mobile support only the Web email clients.

For more information on compatibility of Unity Connection Mini Web Inbox with operating systems and browsers, refer to *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations* available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html .

The administrator can configure Unity Connection to send the voice message as an attachment in the HTML notification to the user. The size of the voice message attachment can also be configured. For more information on how to configure, see the "Configuring Cisco Unity Connection for HTML-based Message Notification" section of the "Configuring an Email Account to Access Cisco Unity Connection Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_setup/guide/10xcucuwsx.html .

The content and format of the HTML notifications received via email can be customized through a notification template, custom variables, and custom graphics. Only the administrator has the rights to create and modify the notification templates, custom variables, and custom graphics. Cisco Unity Connection Administration and the Cisco Unity Connection Provisioning Interface (CUPI) APIs can be used to create, update, and delete the customized notification templates.

For more information on how to manage notification templates through Connection Administration, refer to the "Adding, Modifying, or Deleting a Notification Template in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

For more information on how to manage notification templates using CUPI APIs, refer to the "HTML Notification Templates" section of the Cisco Unity Connection APIs.

To use the HTML notification templates, you must enable the HTML notification device and assign a notification template. Cisco Unity Connection Administration and the CUPI APIs are used to create, update, and delete an HTML notification device. The HTML notification devices can be managed for an individual user, or for multiple users by using the Bulk Edit utility in Cisco Unity Connection Administration.

For more information on how to manage notification devices through Connection Administration, refer to the "Notification Devices in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x* available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

The Unity Connection users can also set up an HTML notification device and configure other settings through the Unity Connection Messaging Assistant Web Tool of Cisco Personal Communications Assistant (PCA). The users also have a choice of using an outdial number to check the voice messages using the telephone record and playback functionality. This facilitates the users to provide their extension or mobile number that gets auto-populated in the Cisco Unity Connection Mini Web Inbox.

The user can access the notified voice message by clicking the hyperlink given in the email for launching the Unity Connection Mini Web Inbox. With Unity Connection Mini Web Inbox, the user can play, reply, reply all, forward, or delete the voice messages using a phone or a computer. On mobile, the Unity Connection Mini Web Inbox is supported via telephone record and playback (TRAP) connections on all native browsers for IPhone.

For more information on Cisco Unity Connection Mini Web Inbox, refer to the *Quick Start Guide for the Cisco Unity Connection Mini Web Inbox* available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/quick_start/guide/b_10xcucqsgminiinbox.html.

**Note** To access the Unity Connection Mini Web Inbox, you must be on the corporate network or connected via VPN to the corporate network. The email notification content including the MWI status, message status, and custom graphics, will be visible through the authentication and/or non-authentication mode when the user is on the corporate network or connected to it using the VPN.

To troubleshoot any issue while creating templates or launching the Unity Connection Mini Web Inbox, refer to the "Troubleshooting the HTML Notifications in Cisco Unity Connection" chapter of the *Troubleshooting Guide for Cisco Unity Connection* available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx.html.

### Receipts

Users can request a read receipt when sending a message. As soon as the recipient listens to the message, the receipt is sent to the message sender. New receipts turn on the message waiting indicator on the user phone and can trigger message notifications.

When a voice message cannot be delivered, if the sender is a user and is configured to accept receipts, Cisco Unity Connection alerts the sender with a nondelivery receipt (NDR). The NDR contains a copy of the original message, which the user can use to resend the message at a later time or to a different recipient.

### Interview Handler Messages

By using interview handlers in your call management plan, you can have Cisco Unity Connection collect information from callers by playing a series of questions that you have recorded, and then recording the answers offered by callers. For example, you might use an interview handler to take sales orders or to gather information for a product support line.

When all the answers have been recorded, they are forwarded as a single voice message, with beeps separating the answers, to the recipient (user or distribution list) that you designate in the interview handler configuration.

See the "Managing Interview Handlers in Cisco Unity Connection 10.x" chapter for more information.

### Dispatch Messages

You can use the dispatch message feature to send a message to a distribution list, with the message configured in such a way that only one user in the group needs to act on the message. When listening to a dispatch message, users are given the option to accept the message, postpone the message, or decline the message. When the message has been accepted by one of the members of the distribution list, the copies in the mailboxes of the remaining recipients are removed.

Dispatch messaging is useful in situations where a team is available to respond to issues, but only one member of the team needs to respond. For example, an IT department may want to set up a call handler to take messages from employees who need assistance, and then send the messages as dispatch messages to a distribution list comprised of IT department staff. All of the members of the distribution list receive a copy of each message. Team members can then decide whether to accept or decline a message.

See the "Dispatch Messages in Cisco Unity Connection 10.x" section on page 22-8 for details.

### Live Record Messages

Live record allows users to record conversations while they talk to callers. The recorded conversation is stored as a message in the user mailbox, and the user can review it later or redirect it to another user or group of users. Operators in your organization may find live record particularly useful.

Live record is supported only when Cisco Unity Connection is integrated with a Cisco Unified Communications Manager phone system.

See the "Configuring Live Record in Cisco Unity Connection 10.x" section on page 22-22 for information on configuring live record.

# Message Recording in Cisco Unity Connection 10.x

Typically, Cisco Unity Connection uses the same audio format (or codec) for recording a message that the playback device uses. For example, if users listen to messages primarily on a phone system extension, Unity Connection should record messages in the same audio format that the phone system uses. If the users listen to messages on Personal Digital Assistants (PDAs), however, Unity Connection should record messages in the audio format that the PDAs use (such as GSM 6.10).

You should consider the following when setting the audio format for recording messages:

- Setting the audio format for recordings affects all messages, greetings, and names systemwide for all users.

- Minimizing the number of different audio formats in use for recording and playing recorded messages, greetings, and names reduces transcoding between audio formats that Unity Connection must perform, and reduces the effect on the performance of the Unity Connection server.
- When a message, greeting, or name is recorded in a lower quality audio format and later transcoded to a higher quality audio format during playback, the sound quality is not improved. Usually, the sound quality of a recording suffers during transcoding, especially when the sampling rate is changed.

  For example, sound quality suffers when messages that are recorded in the G.729a audio format are played on devices that use the G.711 Mu-Law audio format. However, sound quality is preserved when messages that are recorded in the G.711 Mu-Law audio format are played on devices that use the same audio format.
- Changing the audio format for recordings affects only messages, greetings, and names that are recorded after the setting is changed. Existing messages, greetings, and names that were recorded in a different audio format are not affected by the new setting.

#### To Change the Audio Format for Recording Messages

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **Edit General Configuration** page, in the **Recording Format** list, select the applicable setting.

**Note** If the playback device uses a different audio format, Unity Connection must transcode the messages, greetings, and names into the applicable audio format or the playback device is not able to play them.

**Step 3** Select **Save**.

# Configuring the Termination Warning Prompt for the End of Recording

By default, Cisco Unity Connection plays a termination warning prompt before reaching the maximum allowable message length while callers record their messages. (When a recording reaches the maximum allowable message length, the recording session is terminated.) By default, the warning plays 15 seconds before the end of a recording, provided that the recording is not restricted to less than 30 seconds in length. There are two settings that can be customized:

| | |
|---|---|
| **Minimum Recording Duration in Milliseconds for Termination Warning** | The maximum recording length, in milliseconds, before Unity Connection monitors the recording length to determine whether to play the termination warning prompt. This setting prevents the warning from sounding for shorter recordings, for example for interview handlers that are configured to accept only brief responses. |
| **Recording Termination Warning Time in Milliseconds** | The number of milliseconds before reaching the maximum message length when the termination warning prompt is played. A setting of 0 disables the warning. |

For example, if the maximum message length is set for 300 seconds and the **Recording Termination Warning Time in Milliseconds** field is set for 10 seconds, the termination warning prompt is played after 290 seconds of recording—10 seconds before the recording limit is reached and the recording session is terminated. If the **Minimum Recording Duration in Milliseconds for Termination Warning** field is set for 60 seconds, and a call handler is configured with a maximum message length of 30 seconds, callers who reach the call handler and record a message do not hear the warning.

#### To Configure the Termination Warning Prompt for the End of Recording

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Telephony**.

**Step 2** On the **Telephony Configuration** page, in the **Minimum Recording Duration in Milliseconds for Termination Warning** field, enter the minimum length of recordings, in milliseconds, before Unity Connection monitors the recording length to determine whether to play a termination warning prompt.

**Note** The recordings that are not allowed to exceed this length are not monitored by Unity Connection to determine whether to play the warning.

**Step 3** In the **Recording Termination Warning Time in Milliseconds** field, enter the length of time, in milliseconds, before reaching the maximum allowed recording time at which Unity Connection plays a termination warning prompt. When the warning is played during a recording session, Unity Connection continues recording for the amount of time indicated in this field before terminating the recording session.

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

# Default Recipient Accounts in Cisco Unity Connection 10.x

The default Cisco Unity Connection configuration includes several accounts that play a role in message delivery or that receive messages when callers are routed to one of the default system call management objects.

### Operator

When a caller to Cisco Unity Connection dials the operator and no operator is available, the caller can leave a message, depending on the call transfer settings for the **Operator** call handler. By default, messages left in the **Operator** call handler are sent to the voice mailbox of the Operator user. We recommend that you assign someone to monitor this mailbox, or reconfigure the Operator call handler to send messages to a different user or to a distribution list.

During installation, the Operator account is assigned randomly-generated voicemail and web application passwords. To sign in to the account, you must change the passwords by using Cisco Unity Connection Administration.

#### UndeliverableMessagesMailbox

By default, this mailbox is the only member of the **Undeliverable Messages** distribution list. We recommend that you assign someone to monitor this mailbox, or add a user to the Undeliverable Messages distribution list to monitor and reroute (as appropriate) any messages that are delivered to the list. If another user will monitor the distribution list, remove the UndeliverableMessagesMailbox account from the distribution list to prevent the mailbox from filling up with messages.

During installation, the **UndeliverableMessagesMailbox** account is assigned randomly-generated voicemail and web application passwords. To sign in to the account, you must change the passwords by using Cisco Unity Connection Administration.

#### Unity Unity Connection Messaging System

This account acts as a surrogate sender for messages from unidentified callers. Thus, user messages from unidentified callers are identified as coming from the Unity Unity Connection Messaging System mailbox (UnityConnection@<servername>).

The alias for this account is Unity Connection. This account can be viewed in Cisco Unity Connection Administration, but cannot be modified or deleted.

# Dispatch Messages in Cisco Unity Connection 10.x

You can use the dispatch message feature to send a message to a distribution list (from either a call handler or interview handler). The message is configured such that only one user in the group needs to act on the message. When listening to a dispatch message, users are given the option to accept, postpone, or decline the message.

Dispatch messages are handled as follows:

- If a user chooses to accept the message, all other copies of the message are removed from the mailboxes of the other members of the distribution list, regardless of whether the other users have listened to and postponed the message.
- If a user chooses to postpone the message, it remains as an unread message in the mailbox of that user and in the mailboxes of the other members of the distribution list.
- If the user chooses to decline the message, it is removed from the mailbox of that user, but copies of the message remain as unread in the mailboxes of the other members of the distribution list.
- If there is only one copy of the dispatch message remaining, and no user has yet chosen to accept the message, the final user whose mailbox it is in must accept it. That user is not given the option to decline the message.

Dispatch messaging is useful in situations where a team is available to respond to issues, but only one member of the team needs to respond. For example, an IT department may want to set up a call handler to take messages from employees who need assistance, and then send the messages as dispatch messages to a distribution list comprised of IT department staff. All of the members of the distribution list receive a copy of each message. Team members can then decide whether to accept or decline a message; declined messages are then picked up by other team members.

Do one of the following procedures to set up dispatch messaging:

- To Configure Dispatch Messaging for Messages Left for a Call Handler, page 22-9
- To Configure Dispatch Messaging for Messages Left for an Interview Handler, page 22-9

Also see the "Dispatch Messaging Limitations and Behavioral Notes" section on page 22-9.

#### To Configure Dispatch Messaging for Messages Left for a Call Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, in the **System Call Handlers** table, select the display name of the applicable call handler.

**Step 3** On the **Edit Call Handler Basics** page, on the **Edit** menu, select **Message Settings**.

**Step 4** On the **Edit Message Settings** page, under **Message Recipient**, select a distribution list as the recipient and check the **Mark for Dispatch Delivery** check box.

**Step 5** Select **Save**.

#### To Configure Dispatch Messaging for Messages Left for an Interview Handler

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Interview Handlers**.

**Step 2** On the **Search Interview Handlers** page, in the **Interview Handlers** table, select the display name of the applicable interview handler.

**Step 3** On the **Edit Interview Handler Basics** page, under **Recipient**, select a distribution list as the recipient and check the **Mark for Dispatch Delivery** check box.

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

## Dispatch Messaging Limitations and Behavioral Notes

- Only voice messages can be flagged for dispatch. Email and fax messages cannot be flagged for dispatch.
- The handling of dispatch messages is supported only in the phone interface. If a user opens a dispatch message when using the Unity Connection Web Inbox, Cisco Unified Personal Communicator, Cisco Mobile, Cisco Unified Messaging with IBM Lotus Sametime, an IMAP client, or an RSS client, the user is not forced to postpone, decline, or accept the message.Those clients treat dispatch messages as normal voice messages. It is important to make users aware that they must use the phone interface for dispatch messaging to be effective. When using clients other than the phone interface, the only indication that a message is marked for dispatch is when the subject line of the message has been configured to display special text. (For details on configuring subject line formats, see the "Message Subject Line Formats in Cisco Unity Connection 10.x" section on page 22-17.) We recommend that you configure subject line formats to indicate that a message is a dispatch message, as this helps to remind users that they need to access the messages by using the phone interface.
- When single inbox is configured, dispatch messages are not synchronized between Unity Connection and Exchange.
- Dispatch messages are never transcribed, even when the recipients belong to a class of service for which the SpeechView feature is enabled.
- When using an IMAP client to play dispatch messages, it is not possible to delete or mark the messages as read. At first it may appear that a user can successfully delete or save a dispatch message, but the next time the IMAP client refreshes the message list, the dispatch message displays

as a new message. This is true even if the user is using Microsoft Outlook or IBM Lotus Notes with ViewMail. The message is removed only if the user uses the phone interface to decline the message or if another user uses the phone interface to accept the message.

- If there is only one copy of a dispatch message left, it is possible for the user with that last copy to delete it when using the Unity Connection Web Inbox or Cisco Unified Personal Communicator. It is important to make users aware that they must use the phone interface for dispatch messaging to be effective.
- During playback of a dispatch message, if a user presses the phone keypad key that is mapped to the "skip" or "delete" menu options, Unity Connection interprets the "skip" key press as "postpone," and the "delete" key press as "decline."
- Dispatch messages are not sorted separately from normal voice messages. If you want users to hear their dispatch messages first, the call handler or interview handler that is configured to mark the message for dispatch delivery should also be configured to mark the message as urgent. By default, urgent messages are presented to users first.
- If a user declines a dispatch message, a copy of the dispatch message is not kept in the deleted items folder of that user.
- When a user accepts the message, that user is the only person who has a copy of the message in his or her mailbox.
- When a dispatch message is accepted by a user, the dispatch property is removed and it is treated as a normal voicemail message. If the user subsequently saves the message as new, the message is presented in the phone interface just like any other new message and is not announced to the user as a dispatch message. (Note that the subject line is not altered, so depending on the subject line format used, it may contain a string indicating that the message was originally flagged for dispatch. However, the subject line is not played in the phone interface.)
- It is not possible to forward a dispatch message. A user must first accept the message, which removes the dispatch property. Then the user can forward it as a normal voicemail message.
- When configuring message notification rules to include dispatch messages, make users aware that by the time users receive the notification and call in to retrieve the message, it may be gone from their mailboxes because another user has already accepted the message.
- Networked dispatch messages are not supported. Dispatch messaging is not supported across locations. Dispatch messages addressed to recipients at other locations within a site are delivered to remote users as regular messages. Dispatch messages addressed to remote site recipients are not delivered. We recommend that you configure dispatch messaging only when the message recipient is a system distribution list that does not include users on other networked locations.
- If Unity Connection is configured as a cluster, it is possible for two different users to call into the different servers and accept the same dispatch message when more than one server has the Primary status (known as a "split brain" condition). After the split brain condition has been resolved, the user who last accepted the dispatch message becomes the final recipient and the message is removed from the mailbox of the other user.

# Message Delivery in Cisco Unity Connection 10.x

In most cases, Cisco Unity Connection delivers messages from callers by using a standard process—Unity Connection signs in to the sender account (either the Unity Unity Connection Messaging System account for unidentified caller messages, or the user voice mailbox), composes and addresses the message to the recipient or to the members of the recipient distribution list, and delivers the message.

See the following sections for detailed information on message delivery issues:

- How Cisco Unity Connection Handles Messages That Cannot Be Delivered, page 22-11
- How Cisco Unity Connection Handles Messages When System Components Are Unavailable, page 22-11
- How Cisco Unity Connection Handles Messages That Are Interrupted by Disconnected Calls, page 22-12
- How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded, page 22-13
- How Cisco Unity Connection Handles Messages When Maximum Mailbox Store Size Is Exceeded, page 22-14

# How Cisco Unity Connection Handles Messages That Cannot Be Delivered

Occasionally, messages cannot be delivered to the recipient that the caller intended to reach. The system behavior in this case depends on the type of sender and the reason that the message could not be delivered.

In general, if Cisco Unity Connection cannot deliver the message because of issues that are not likely to be resolved (for example, the caller was disconnected before addressing the message, or the recipient mailbox has been deleted), the message is sent to the Undeliverable Messages distribution list, and Unity Connection sends a nondelivery receipt (NDR) to the sender.

Note that the sender does not receive a nondelivery receipt in the following cases:

- When the sender of the original message is an unidentified caller
- When the sender is a user, but the user account is configured not to accept NDRs
- While the mailstore of the user is offline (in this case, the NDR is delivered when the database becomes available)

However, if the original message is malformed, instead of sending the message to the Undeliverable Messages list, Unity Connection places the message in the MTA bad mail folder (UmssMtaBadMail). This folder is automatically checked nightly by the **Monitor Bad Mail Folders** task, and if messages are found, an error is written to the application event log indicating troubleshooting steps.

# How Cisco Unity Connection Handles Messages When System Components Are Unavailable

During temporary outages, the system behavior depends on the nature of the outage.

### Message Delivery Components

If the components involved in message delivery on the Cisco Unity Connection server are unavailable (if the mailbox store is disabled because it is being backed up, for example), Unity Connection queues any messages that are recorded by users or outside callers, and delivers them when the component becomes available.

When single inbox is configured, messages queued for delivery are not synchronized with Exchange mailboxes while components are unavailable. After the messages are delivered, they are also synchronized with Exchange mailboxes.

### Exchange Is Unavailable

If Unity Connection is configured to allow users access to email messages in Exchange, and network or other conditions slow or prevent responses when Unity Connection attempts to retrieve messages from Exchange, Unity Connection announces to users that email is unavailable when they attempt to access email messages. The time period that Unity Connection waits for a response from Exchange defaults to four seconds, and is configurable in Cisco Unity Connection Administration.

When single inbox is configured, Unity Connection messages are not synchronized with Exchange, but users are not notified. When Exchange is available again, synchronization resumes.

Do the applicable procedure to change the length of the timeout:

- To Change the Timeout Period That Cisco Unity Connection Waits for a Response from Exchange
- To Change the Timeout Period That Cisco Unity Connection Waits for a Response from Exchange

#### To Change the Timeout Period That Cisco Unity Connection Waits for a Response from Exchange

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **Unified Messaging Services**.

**Step 2** On the **Unified Messaging Services Configuration** page, change the **TTS and Calendars: Time to Wait for a Response (In Seconds)** setting to the desired value. The setting default is 4 seconds.

**Step 3** Select **Save**.

The change takes effect immediately.

#### To Change the Timeout Period That Cisco Unity Connection Waits for a Response from Exchange

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **External Services**.

**Step 2** On the **External Services Configuration** page, change the **Maximum External Service Response Time (in Seconds)** setting to the desired value. The setting default is 4 seconds.

**Step 3** Select **Save**.

The change takes effect immediately.

# How Cisco Unity Connection Handles Messages That Are Interrupted by Disconnected Calls

You can change how Cisco Unity Connection handles messages that are interrupted by disconnected calls while users are in the process of sending, replying to, or forwarding messages. Calls can be intentionally or unintentionally disconnected—for example, when a user hangs up or when a mobile phone loses its charge or signal.

By default, Unity Connection sends a message when the call is disconnected in the following circumstances:

| | |
|---|---|
| **When a user is replying to or sending a message** | As long as the message has at least one recipient and the recording is more than one second (1,000 milliseconds) in length. This means that Unity Connection sends the message even though the user may not have finished recording or addressing the message. |
| **When a user is forwarding a message** | As long as the message has at least one recipient. This means that Unity Connection sends the message even though the user may not have recorded an introduction or completely addressed the message. |

You can configure Unity Connection to delete interrupted messages unless users have pressed the # key to send their messages. Thus, if a call is disconnected before a user has a chance to press #, Unity Connection deletes the message rather than sending it. Note that the setting can be configured per user. For details, see the "Specifying Whether Messages Are Sent Upon Hang-Up" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# How Cisco Unity Connection Handles Messages When Mailbox Quotas are Exceeded

Message handling when send or send/receive quotas have been exceeded depends on whether the sender is an outside caller or a user.

### Quota Handling for Outside Caller Messages

By default, if an outside caller attempts to send a message to a user whose send/receive quota has been exceeded, Cisco Unity Connection allows the caller to record a message for the recipient. You can change this behavior by checking the **Full Mailbox Check for Outside Caller Messages** check box on the **System Settings > Advanced > Conversation** page.

If the recipient mailbox has not yet exceeded the send/receive quota at the time an outside caller records a message, but the quota is exceeded in the act of delivering the message, Unity Connection delivers the message regardless of the quota or the setting of the **Full Mailbox Check for Outside Caller Messages** check box.

### Quota Handling for User-to-User Messages

If a user whose voice mailbox has exceeded the send quota signs in to Unity Connection and attempts to send a message to another user, Unity Connection indicates that the send quota has been exceeded, and does not allow the sender to record the message. If the user calls another user and is forwarded to a voice mailbox, the user is able to leave a message, but the message is sent as an outside caller message.

If a user attempts to send a message to another user whose mailbox has exceeded the send/receive quota, or if the quota is exceeded in the act of delivering the message, Unity Connection sends a nondelivery receipt to the message sender.

Unity Connection delivers read receipts and nondelivery receipts to users regardless of whether their quotas have been exceeded.

## How Cisco Unity Connection Handles Messages When Maximum Mailbox Store Size Is Exceeded

When you create a mailbox store, you specify a maximum size for the store, which is a sum of the sizes of all of the mailboxes in that store. If a mailbox store reaches 90 percent of the maximum size, Cisco Unity Connection logs a warning. If a mailbox store reaches 100 percent of the maximum size, Unity Connection logs an error. (The warning and error messages can be viewed in the Real-Time Monitoring Tool.) However, Unity Connection functionality is not affected. You can continue to add or move mailboxes to a mailbox store that has reached the maximum size, and Unity Connection continues to take messages for users whose mailboxes are in a mailbox store that has reached the maximum size.

For more information on managing mailbox stores, see the "Managing Mailbox Stores in Cisco Unity Connection 10.x" chapter.

# Message Delivery and Sensitivity Options in Cisco Unity Connection 10.x

Message delivery and sensitivity options allows administrators and users to control when a message is delivered, who can access it, and whether it can be redistributed to others. In some cases, message sensitivity can also prevent users from saving a voice message to their hard drives or other locations outside the Cisco Unity Connection server.

Unity Connection offers the following message delivery and sensitivity options for users and outside callers:

| | |
|---|---|
| **Urgent** | Urgent messages are delivered before normal messages.<br><br>Users who are signed in to their mailboxes can always mark a message urgent. When unidentified callers and users who have not explicitly signed in to their mailboxes leave messages for users or call handlers, they can mark the message urgent only if the user account or call handler is set up to allow them to do so on the **Edit >Message Settings** page. |

| | |
|---|---|
| **Private** | A private message can be sent to anyone, but the message cannot be forwarded by a recipient listening to it by using the following interfaces:<br>• Phone<br>• Unity Connection Web Inbox<br>• Unity Connection Messaging Inbox<br>• ViewMail for Outlook<br>• ViewMail for Notes<br>Recipients who listen to a private message via an IMAP client (including Microsoft Outlook when ViewMail for Outlook is not installed) can forward the message, and can save it as a .wav file. (See the "Message Security Options for IMAP Client Access in Cisco Unity Connection 10.x" section in the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x* to learn how to prevent this. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.)<br>User-to-user messages can be marked private. Outside callers and users who have not explicitly signed in to their mailboxes cannot mark a message private. When outside callers and users who have not explicitly signed into their mailboxes leave messages for users or call handlers, they can mark the message private if the user account or call handler is set up to allow them to do so. |
| **Secure** | Only Unity Connection users can receive a secure message. The message can be played and forwarded by using the following interfaces:<br>• Phone<br>• The Unity Connection Web Inbox<br>• The Messaging Inbox<br>• Cisco Unity Connection ViewMail for Microsoft Outlook 8.5<br>The message can be played but not forwarded by using the following methods:<br>• Cisco Unity Connection ViewMail for Microsoft Outlook 8.0<br>• Cisco Unity Connection ViewMail for IBM Lotus Notes<br>The message cannot be accessed by using an IMAP client other than Microsoft Outlook with ViewMail or Lotus Notes with ViewMail.<br>The message cannot be saved locally as a WAV file.<br>User-to-user messages can be marked secure only when the user class of service settings allow it. Outside callers and users who are not explicitly signed in to their mailboxes cannot mark a message secure. Instead, the **Mark Secure** check box on the **Edit > Message Settings** page for a user account or call handler determines whether Unity Connection automatically marks messages from outside callers secure, or delivers them with normal sensitivity. |

| | |
|---|---|
| **Future Delivery** | After addressing and recording a message by using the touchtone conversation or the voice-recognition conversation, a user can mark the message for future delivery so that Unity Connection waits to send the message on the day and time that the user specifies. Once future delivery is set on the message, the user can cancel the future delivery as long as the user has not yet chosen the option to send the message.<br><br>In the event of an urgent need, administrators can cancel all pending messages that are set for future delivery by using the "delete cuc futuredelivery" CLI command. Note, however, that there is no administrative option to cancel any specific messages after they have been sent by the user. |

The "How Cisco Unity Connection 10.x Handles Messages That Are Marked Private or Secure" section in the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x* details how Unity Connection handles private and secure messages. (The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.)

# Message Actions in Cisco Unity Connection 10.x

Cisco Unity Connection uses the message action settings for a user to determine how to handle the different types of messages that it receives for the user. The message action setting for a particular type of message (voice, email, fax, or delivery receipt) affects all messages of that type that are sent to or created on the Unity Connection server from any client (for example, by using the phone interface, the Unity Connection Messaging Assistant, or an IMAP client).

By default, Unity Connection is configured to accept each type of message, an action that causes Unity Connection to place the message in the user mailbox in the applicable Unity Connection mailbox store.

You can use the relay action to instruct Unity Connection to send all messages of a certain type to a different messaging system, such as a corporate email server, for storage and user access. (This is sometimes referred to as message forwarding.) If you choose this option, users are no longer able to access these types of messages from the Unity Connection phone interface, from the Messaging Assistant, or from other clients such as Phone View or Cisco Unified Personal Communicator. (The exception is relaying email messages to an external message store to which Unity Connection is configured to connect so that users can hear their emails read to them when they sign in to Unity Connection by phone.) You configure one or more message actions to relay messages to a single SMTP relay address for the user, which you define on the Message Actions page for the user. (You can also configure Message Actions for user templates, or for multiple users at once in Bulk Edit mode; in these cases, you can use a combination of text and replaceable tokens to define a template for the SMTP address, from which Unity Connection creates a relay address for each individual user.) Note that Unity Connection relays messages through an SMTP smart host, and you must have the smart host configured on the Unity Connection server before you can configure this action for a user or user template.

You can use the accept and relay action to instruct Unity Connection to both deliver each message of a certain type to the user mailbox and forward a copy of the message to the relay address. (This is sometimes referred to as "accept and forward.") This option may be useful for users who regularly use a device that accesses a separate server for messages, such as a handheld wireless device, and want easy access to voice messages both on the alternative device and through the Unity Connection user interfaces. If you choose this option, the user receives two copies of each message. The copies are stored in different message stores, and any actions the user takes on the relayed copy are not reflected on the copy stored in the Unity Connection message store. Note that if the user does not regularly manage new messages in the Unity Connection message store, the user mailbox may quickly exceed the mailbox quota because new messages are not subject to message aging policies.

You can use the reject action to instruct Unity Connection to discard all messages of a particular type that a user receives and send a non-delivery receipt to the message sender.

# Message Subject Line Formats in Cisco Unity Connection 10.x

Message subject lines are visible when users view and listen to messages in the Cisco Unity Connection Web Inbox, Unity Connection Messaging Inbox, an IMAP client, an RSS client, or any other visual client that displays the message subject. Subject lines are not presented to users when they listen to voice messages by phone.

You can configure both the wording and the information that is included in the subject line of voice messages, including localizing the subject line according to the language of the recipient.

The subject lines of the following message types can be defined:

- **Outside Caller Messages**—Messages from callers who are not Cisco Unity Connection users, and also from Unity Connection users who send messages without first signing in to Unity Connection or who have not been automatically identified as Unity Connection users by the **Identified User Messaging** feature. This includes messages that are left for a system call handler.
- **User to User Messages**—Messages from callers who have either signed in to Unity Connection, or have been automatically identified as Unity Connection users because **Identified User Messaging** is enabled. This includes messages that are left from users for a system call handler.
- **Interview Handler Messages**—Messages that are left for interview handlers.
- **Live Record Messages**—Messages containing conversations that users recorded while they talked to callers.

**Note** Subject lines for call handler messages use the definition of outside caller messages or user to user messages, depending on whether the call handler message is from an outside caller or a user.

See the following sections for additional information:

- Subject Line Parameters, page 22-17
- Subject Line Format Examples, page 22-19
- Subject Line Format Configuration, page 22-19

## Subject Line Parameters

Table 22-1 describes the parameters that can be used to define message subject lines.

*Table 22-1 Parameters Used to Define Message Subject Lines*

| Parameter | Description |
|---|---|
| %CALLERID% | When the %CALLERID% parameter is used in a subject line format, it is automatically replaced with the ANI Caller ID of the sender of the message.<br><br>If the ANI Caller ID is not available, the text entered in the %CALLERID% (When Unknown) field is inserted into the subject line instead. |

*Table 22-1 Parameters Used to Define Message Subject Lines (continued)*

| Parameter | Description |
|---|---|
| %CALLEDID% | When the %CALLEDID% parameter is used in a subject line format, it is automatically replaced with the ID of the number called by the sender of the message. If the Called ID is not available, the text entered in the %CALLEDID% (When Unknown) field is inserted into the subject line instead.<br><br>You might find this field useful in cases where more than one organization shares a single Cisco Unity Connection system, and there are multiple inbound numbers defined so that callers can be routed to different opening greetings. In this case it might be helpful if messages left in a general help voice mailbox include the number that the sender of the message used when calling the system. |
| %NAME% | When the %NAME% parameter is used in the subject line format of an outside caller message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Cisco Unity Connection inserts the value specified in the %NAME% (When Unknown) field.<br><br>When the %NAME% parameter is used in the subject line format of a user to user message, it is automatically replaced with the display name of the sender of the message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field.<br><br>When the %NAME% parameter is used in the subject line format of an interview handler message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Unity Connection inserts the display name of the interview handler. If the display name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field.<br><br>When %NAME% is used in the Live Record Messages field, it is automatically replaced with the display name of the user who initiated the live record message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field. |
| %EXTENSION% | When the %EXTENSION% parameter is used in a subject line format, it is automatically replaced with the extension of the sender of the message, or for messages recorded by call handlers or interview handlers, with the extension of the handler.<br><br>If the extension is not available, the value entered in the %EXTENSION% (When Unknown) field is inserted into the subject line instead.<br><br>**Note** When %EXTENSION% is used in the Live Record Messages field, it is replaced with the extension of the user who initiated the live record message. |
| %U% | When the %U% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %U% field if the message is flagged as urgent. If the message is not urgent, this parameter is omitted. |
| %P% | When the %P% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %P% field if the message is flagged as private. If the message is not private, this parameter is omitted. |
| %S% | When the %S% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %S% field if the message is flagged as a secure message. If the message is not a secure message, this parameter is omitted. |
| %D% | When the %D% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %D% field if the message is flagged as a dispatch message. If the message is not a dispatch message, this parameter is omitted. |

# Subject Line Format Examples

*Table 22-2 Subject Line Format Examples*

| Type of Message | Subject Line Format | Message Details | Subject Line of the Message Received |
|---|---|---|---|
| Outside caller message | %U% %D% Voice message from %CALLERID% | An outside caller with the ANI Caller ID 2065551212 | "Voice message from 2065551212" |
| User to user message | %U% %P% %S% Message from %NAME% [%CALLERID%] | John Jones, at extension 4133—an urgent message | "Urgent Message from John Jones [4133]" |
| Interview handler message | Message from %NAME% [%CALLERID%] | "Sales Survey" interview handler, no ANI caller ID available | "Message from Sales Survey [Unknown caller ID]" |
| Live Record message | Live Record message from %CALLERID% | User recording of a phone call from a caller with the ANI caller ID 4085551212 | "Live Record message from 4085551212" |

# Subject Line Format Configuration

You should consider the following when defining subject line formats:

- You must include a % before and after the parameter.
- You can define a separate subject line format for each language that is installed on the system.
- When a subject line format is not defined for the preferred language of the user, the subject line format definition for the system default language is used instead.
- When a message is sent to a distribution list, the subject line format for the system default language is used for all recipients on the distribution list. This means that the subject line is not necessarily in the preferred language of each recipient.
- There is no parameter with which to indicate that a message is being sent to a distribution list.
- Subject line formats are applied to voice messages when the messages are saved to the database. Messages that are already in user mailboxes are not altered if the subject line format definitions are subsequently changed. Only voice messages that are recorded after the changes have been saved reflect the new subject line definition.

Do the following procedure to configure subject line formats.

### To Configure Subject Line Formats

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Subject Line Formats**.

**Step 2** On the Edit Subject Line Formats page, select the applicable language.

**Step 3** Enter text and parameters in the Subject Line Formats fields, as applicable. For descriptions of the available parameters, see Table 22-1.

**Step 4** Enter text in the Parameter Definitions fields, as applicable.

**Step 5** Select **Save**.

The information you enter affects the subject lines of any new voice messages. The subject line formats are not applied to messages that are already in user mailboxes.

**Step 6** Repeat Step 2 through Step 5 as needed for additional languages.

# Message Storage and Disk Capacity in Cisco Unity Connection 10.x

Cisco Unity Connection stores message content as files on the Unity Connection server, and stores information about the messages in a database.

Depending on the number of Unity Connection users, the number and duration of messages they receive, and the settings that you specify for the message aging policy and for quotas, it may be possible for the hard disk on which messages and greetings are stored to fill up. This would cause Unity Connection to stop functioning. As the hard disk approaches maximum capacity, you may also encounter unexpected behavior.

On the Disk Capacity page (**System Settings > Advanced > Disk Capacity** in Cisco Unity Connection Administration), you can specify a maximum capacity for the hard disk on which messages and greetings are stored. When the hard disk fills to the specified percentage limit, neither Unity Connection users nor outside callers are allowed to leave voice messages. Unity Connection also logs an error, which can be viewed on the **Tools > SysLog Viewer** page in the Real-Time Monitoring Tool. Note that you can still send a broadcast message even when the hard disk exceeds the specified limit.

We recommend that you specify a value no greater than 95 percent. If you change the disk-capacity setting, use Cisco Unity Connection Serviceability to restart the Unity Connection Message Transfer Agent service.

If the hard disk exceeds the value that you specify, instruct Unity Connection users to immediately delete unneeded voice messages. In addition, to prevent a recurrence, you may want to reevaluate message-aging policy and mailbox quotas. For more information, see the "Controlling the Size of Mailboxes in Cisco Unity Connection 10.x" chapter.

**Note** For ways to prevent users from saving messages as WAV files to their hard drives or other locations outside of the Unity Connection server, see the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.

# Deleting Messages in Cisco Unity Connection 10.x

In Cisco Unity Connection, there are multiple methods that users can use to delete messages. In addition, there are configuration settings that system administrators can use to manage the deletion of messages to meet the disk capacity needs and security needs of an organization. See the following sections:

- Soft Deletes and Hard Deletes, page 22-21
- Deleting Messages by Way of Message Aging Policies, page 22-21
- Message File Shredding for Secure Deletes, page 22-22

# Soft Deletes and Hard Deletes

In Cisco Unity Connection, messages can be either “soft” or “hard” deleted. Depending on how you choose to set the Delete Messages Without Saving to Deleted Items Folder class of service setting, user actions to delete messages will result in the messages being moved to a deleted items folder (“soft” deletes), or being permanently deleted (“hard” deletes).

When messages are soft deleted, for example when a user deletes a message after listening to the message by phone, or deletes it in the Unity Connection Web Inbox or Messaging Inbox, the message is marked as deleted in the Unity Connection database, and is moved to the **Deleted Items** folder. As long as the message is still in the **Deleted Items** folder, it is still recoverable by the user. The user can listen to deleted voice messages; retrieve the deleted messages to reply to them or forward them; restore them to the Inbox; or delete them permanently by hard deleting them.

When the **Delete Messages Without Saving to Deleted Items Folder** check box is checked to enable it, all user deletes will be hard deletes.

When the Delete Messages Without Saving to Deleted Items Folder setting is not enabled, the user needs to use one of the following methods to hard delete a message:

- The user signs in to Unity Connection by phone. From the **Main** menu, the user selects the option to Review Old Messages, then selects Deleted Messages, and then follows the prompts to permanently delete individual messages or all old messages.
- To hard delete a message in the Web Inbox or Messaging Inbox, the user clears the deleted items folder.
- To hard delete a message in an IMAP client application, the user expunges deleted messages.

For more information about the **Delete Messages Without Saving to Deleted Items Folder** class of service setting, see the “Deleted Message Access in Cisco Unity Connection 10.x” section in the “Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 10.x” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

**Note** Make sure that the “Hard” delete option is enabled to delete files permanently from the system. If the "Hard" delete option is not enabled, the files that you delete are moved to the deleted items folder. The files are not deleted from the deleted items folder until they are explicitly deleted, or deleted through aging rules.

# Deleting Messages by Way of Message Aging Policies

To permanently delete messages without any action required from the users who received them, you can configure message aging policies. For example, you can configure a message aging policy to automatically move read messages to the deleted items folder a specified number of days after they are read, and configure another message aging policy to permanently delete messages that are in a deleted items folder a specified number of days after they are moved to the folder. (Note that the default voicemail user template is assigned to a default system message aging policy that automatically cleans up the **Deleted Items** folder after 15 days.) For detailed information on configuring message aging policies, see the “Managing Message Aging Policies in Cisco Unity Connection 10.x” section on page 26-4.

## Message File Shredding for Secure Deletes

The Message File Shredding Level setting on the Advanced Settings > Messaging Configuration page in Cisco Unity Connection Administration is a systemwide setting that ensures copies of messages are securely deleted, by shredding the messages the specified number of times when they are deleted. The shredding is done by way of a standard Linux shred tool: the actual bits that make up the message are overwritten with random bits of data the specified number of times. Note that messages are shredded only when they have been hard deleted.

Cisco Unity Connection uses RAID technology to provide disk redundancy on the server. The RAID technology covers all the disk faults by working from a healthy disk until the faulty disk is rebuilt. As the RAID technology hides the disk errors from the operating system and performs optimizations, the shredding might not work properly in some potential scenarios. The following are some of the instances where shredding does not work properly:

- Disk mirroring during normal operation: Based on the RAID hardware, the RAID technology optimizes the mirroring and waits for the data to be finalized before committing it to the mirror drive. As per the RAID 1 specification, the **Write** command must be sent to all the disks. However, some manufacturers do not follow the RAID 1 specification and the **Write** command is not sent to all the disks. For example, if shred performs 25 overwrites on some data on disk 1, it is not necessary that all the overwrites are performed on disk 2 also. In such cases, the RAID controller might wait for the completion of writes on disk 1, and then it mirrors over the final data on disk 2.
- Disk mirroring during a disk rebuild: If disk 1 gets corrupted, it can be rebuilt with the information stored on disk 2. In such case, the areas shredded on disk 2 will only be recovered instead of the data shredded on disk 1.

For detailed information on secure deletes, see the "Shredding Message Files for Secure Delete in Cisco Unity Connection 10.x" section in the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.

# Message Access in Cisco Unity Connection 10.x

Unity Connection users can always access their new and saved voice messages by phone by using a touchtone or voice-recognition conversation. You specify whether users can access their deleted messages.

Depending on their class of service settings, users may also gain access to voice messages from other applications, such as the Cisco Unity Connection Web Inbox, Unity Connection Messaging Inbox, the Cisco Personal Communicator, or an RSS reader. When set up to do so, users can access Unity Connection voice messages from an IMAP client, Cisco Unified Messaging with IBM Lotus Sametime, or an RSS reader.

Finally, depending on their external service or unified messaging service accounts, users may access email messages in an external message store by phone.

# Configuring Live Record in Cisco Unity Connection 10.x

Live record allows users to record conversations while they talk to callers. The recorded conversation is stored as a message in the user mailbox, and the user can review it later or redirect it to another user or group of users. Operators in your organization may find live record particularly useful.

Live record is supported only for Cisco Unified Communications Manager integrations.

While there is no class of service or user account setting required to enable the feature, note that the maximum duration of a live record message is controlled by the maximum message length for the class of service of the user. In addition, live record does not work for users who have full mailboxes. When a user who has a full mailbox tries to record a call, the feature seems to work normally, but the recorded conversation is not stored as a message in the user mailbox.

Do the following procedures in the order given.

#### To Add a Live Record Pilot Number to Cisco Unified Communications Manager

**Step 1** In Cisco Unified CM Administration, on the Call Routing menu, select **Directory Number**.

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

**Step 3** On the **Directory Number Configuration** page, in the **Directory Number** field, enter the directory number of the live record pilot number. For example, enter "5110."

**Step 4** In the **Route Partition** field, select the partition that contains all voicemail port directory numbers.

**Step 5** In the **Description** field, enter **Live Record** or another description.

**Step 6** In the **Voice Mail Profile** field, accept the default of **None**.

**Step 7** In the **Calling Search Space** field, select the calling search space that includes the partition that you selected in Step 4.

**Step 8** In the **Forward All** field, under **Destination**, enter the voicemail pilot number for the Cisco Unity Connection voice messaging ports.

**Step 9** In the **Forward All** field, under **Calling Search Space**, select the calling search space that includes the partition that you selected in Step 4.

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

The following procedure is optional. It configures Cisco Unified CM so that all parties in a conference call are disconnected when the initiator hangs up. Otherwise, Cisco Unity Connection remains connected until the last party on the call hangs up.

#### To Configure Cisco Unified Communications Manager Conference Settings (Optional)

**Step 1** In Cisco Unified CM Administration, on the **System** menu, 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 - Conference)**, in the **Drop Ad Hoc Conference** field, select **When Conference Controller Leaves**.

**Step 5** Select **Save**.

### To Create a Call Routing Rule for Live Record in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **Call Routing > Forwarded Routing Rules**.

**Step 2** On the **Forwarded Routing Rules** page, select **Add New**.

**Step 3** On the **New Forwarded Routing Rule** page, in the **Description** field, enter **Live Record** or another descriptive name and select **Save**.

**Step 4** On the **Edit Forwarded Routing Rule** page, in the **Status** field, select **Active**.

**Step 5** Under **Send Call To**, select **Conversation**.

**Step 6** In the **Conversation** list, select **Start Live Record**.

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

**Step 8** Under **Routing Rule Condition**, select **Add New**.

**Step 9** On the **New Forwarded Routing Rule Condition** page, select **Forwarding Station**.

**Step 10** To the right of the **Forwarding Station** option, select **Equals** and enter the live record pilot number that you created in the "To Add a Live Record Pilot Number to Cisco Unified Communications Manager" procedure on page 22-23. For example, enter "5110."

**Step 11** Select **Save**.

The following procedure is optional. It adjusts the interval between beeps while Cisco Unity Connection is recording a phone conversation.

### To Adjust the Live Record Beep Interval (Optional)

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Telephony**.

**Step 2** On the **Telephony Configuration** page, in the **Live Record Beep Interval in Milliseconds** field, enter the interval (in milliseconds) between beeps when a phone conversation is being recorded by using the live record feature.

If the setting is blank, the interval is 15,000 milliseconds. If the setting is 0, the beep is disabled.

**Step 3** Select **Save**.

### To Test Live Record

**Step 1** From a user phone, dial an extension.

**Step 2** After the dialed extension is answered, on the user phone, press the **Confrn** softkey to start a conference call.

**Step 3** Dial the live record pilot number that you created in the "To Add a Live Record Pilot Number to Cisco Unified Communications Manager" procedure on page 22-23. For example, dial "5110."

**Step 4** To join the Unity Connection live recorder with the conference call, press the **Confrn** softkey.

**Step 5** After recording the phone conversation, hang up the user phone.

**Step 6** On the user phone, sign in to the voice mailbox for the user.

**Step 7** Listen to the recorded phone conversation.

# Configuring Access to RSS Feeds of Voice Messages in Cisco Unity Connection 10.x

As an alternative to checking messages by phone or using the Cisco Unity Connection Web Inbox, Unity Connection Messaging Inbox, or an IMAP client, users can retrieve voice messages by using an RSS reader. In order to use the RSS Feed feature, users must be assigned to a class of service that is configured to allow them to use the Messaging Inbox and RSS Feeds, and the Unity Connection Inbox RSS Feed service must be turned on and started. Do the following procedure.

**Note** RSS feeds support both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Unity Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrug051.html.

### To Confirm That the Inbox RSS Feed Service Is Turned On and Started

**Step 1** In Cisco Unity Connection Serviceability, select **Tools > Service Management**.

**Step 2** In the **Optional Services** section, confirm that the **Unity Connection Inbox RSS Feed** service is turned on and started.

See the following sections for additional details on configuring access to RSS Feeds:

- Allowing Insecure Connections to RSS Feeds, page 22-25
- Configuring an RSS Reader to View Voice Messages, page 22-26
- RSS Feed Limitations and Behavioral Notes, page 22-26

## Allowing Insecure Connections to RSS Feeds

By default, Cisco Unity Connection only supports secure connections to the RSS feed, using SSL. Some RSS readers, such as Apple iTunes, do not support secure connections.

If you want to allow users to be able to use RSS readers that do not support secure connections, do the following procedure.

### To Allow Insecure RSS Connections

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced > RSS**.

**Step 2** On the **RSS Configuration** page, check the **Allow Insecure RSS Connections** check box.

**Note** When you use an RSS reader that does not support secure connections, if this check box is checked, the username and password are transmitted unencrypted over the network.

**Step 3** Select **Save**.

# Configuring an RSS Reader to View Voice Messages

Users can configure an RSS reader to view voice messages. For instructions on how to set up the RSS reader, refer to the documentation for your reader.

Note these general guidelines:

- Use the following URL in the RSS Reader:
  - https://<Unity Connection server name>/cisco-unity-rss/rss.do

**Note** The Unity Connection server name can be either the Hostname, IPv4 address, or IPv6 address of the Unity Connection server. However, the IPv6 address works only when Unity Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrug051.html.

- When users connect to the RSS feed, they are required to provide the following:
  - User Name—Enter the user alias.
  - Password—Enter the Cisco PCA password of the user (also known as the web-application password).

# RSS Feed Limitations and Behavioral Notes

- Only the 20 most recent unread messages are presented in the RSS feed.
- If the message is secure or private, a decoy message plays instead of the actual message. The decoy message indicates that the message is secure or private and that the user must retrieve the message by calling in by phone.
- Broadcast messages are not included in the RSS feed.
- Messages cannot be deleted. Messages can only be marked read.
- Marking a message read removes it from the RSS feed.
- US English is the only language supported at this time.
- Dispatch messages cannot be accepted, declined or postponed. Dispatch messages cannot be marked as read. A dispatch message remains in the RSS feed until it is handled via another interface or accepted by another recipient.
- Some RSS readers, such as Apple iTunes, do not allow the description of the message to contain hyperlinks. For those readers, the feed does not offer the option to mark the message as read.

- For messages with multiple parts (for example a forwarded message with an introduction), not all parts of the message can be played. Only the first part (for example, the introduction) is played and the subject line indicates that there are more attachments. Users must retrieve the remaining message parts by calling in by phone.

# Configuring IMAP Settings in Cisco Unity Connection 10.x

This chapter contains information on setting up Cisco Unity Connection so that users can use IMAP clients to send, forward, or reply to messages through the Unity Connection server.

See the following sections:


- Overview of SMTP Message Handling in Cisco Unity Connection 10.x, page 23-1
- Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook 10.x, page 23-2
- Recommendations for Deploying IMAP Access in Cisco Unity Connection 10.x, page 23-3
- Task List for Configuring IMAP Access in Cisco Unity Connection 10.x, page 23-3
- Procedures for Configuring IMAP Access in Cisco Unity Connection 10.x, page 23-5


## Overview of SMTP Message Handling in Cisco Unity Connection 10.x

Cisco Unity Connection can receive and process SMTP messages that are generated by IMAP clients, for example, a voice message recorded in a Microsoft Outlook email client by using ViewMail for Outlook.

When an authorized IMAP client tries to send a message to Unity Connection through SMTP, Unity Connection attempts to categorize the message as a voicemail, email, fax, or delivery receipt. Unity Connection also attempts to map the sender to a user and the message recipients to users or contacts by comparing the SMTP addresses in the message header to its list of SMTP proxy addresses.

If SMTP authentication is configured for the IMAP client and the SMTP address of the sender matches a proxy address or the primary SMTP address for the authenticated user, or if SMTP authentication is not configured for the IMAP client and the SMTP address of the sender matches a proxy address or primary SMTP address for any Unity Connection user, Unity Connection processes the message for each individual recipient based on the type of recipient:

- If the recipient maps to a VPIM contact, Unity Connection converts the message into a VPIM message, removing any attachment that is not allowed by the VPIM standard. Then, Unity Connection either delivers the message to the specified VPIM location if the VPIM location is homed on the local server, or forwards it to another digitally networked Unity Connection server for delivery if the VPIM location is homed on that server.

- If the recipient maps to a user homed on the local server, Unity Connection performs the action specified on the Message Actions page of the profile for the user in Cisco Unity Connection Administration. For each type of message (voice, email, fax, or delivery receipt) you can configure whether Unity Connection accepts the message and places it in the user mailbox on the Unity Connection server, relays the message to the user at an alternate SMTP address, or rejects the message and generates a non-delivery receipt (NDR).
- If the recipient maps to a user homed on a remote Unity Connection server, Unity Connection relays the message to the home server of the user, which then performs the action specified on the Message Actions page of the user profile.
- If the recipient does not map to any of the above, Unity Connection either relays the message to the SMTP smart host, or sends an NDR to the sender, depending on the option selected for the When a Recipient Cannot be Found setting on the System Settings > General Configuration page in Connection Administration. By default, Unity Connection sends an NDR.

If SMTP authentication is configured for the IMAP client and the SMTP address of the sender does not match a proxy address or the primary SMTP address for the authenticated user, the Unity Connection server returns an SMTP error, which in most cases causes the message to remain in the client outbox. If SMTP authentication is not configured for the IMAP client and the SMTP address of the sender does not match any known user proxy address or primary SMTP address, Unity Connection puts the message into the MTA bad mail folder (UmssMtaBadMail).

**Note** Unity Connection marks an incoming SMTP message as secure if the message includes the secure header, or if the message sender is a user who is in a class of service that is configured to always send secure messages. See the "How Cisco Unity Connection 10.x Handles Messages That Are Marked Private or Secure" section in the "Securing User Messages in Cisco Unity Connection 10.x" chapter of the *Security Guide for Cisco Unity Connection Release 10.x at* http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx.html.)

# Example Using IMAP and Cisco Unity Connection ViewMail for Microsoft Outlook 10.x

The employees at ExampleCo use Microsoft Outlook to access a Microsoft Exchange server for email. Each employee at the company receives corporate email at an address that follows the pattern firstname.lastname@example.com. ExampleCo wants employees to be able to use Outlook to access voice messages stored on the Cisco Unity Connection server. To allow employees to send, forward, or reply to voice messages in the Outlook client, ExampleCo deploys the Cisco Unity Connection ViewMail for Microsoft Outlook plug-in. The Outlook client for each employee is configured to access the Unity Connection user account via IMAP.

When Robin Smith at ExampleCo wants to send an email message to a coworker, Chris Jones, Robin composes a new email message to chris.jones@example.com. By default, Outlook is configured to route new email messages to the Microsoft Exchange server for delivery. Next, Robin wants to send Chris a voice message, and selects the **New Voice Message** icon, which opens the ViewMail for Outlook form. Robin again addresses the message to chris.jones@example.com, records audio for the message, and selects the Send button. In this case, because ViewMail is configured to use the Unity Connection IMAP account to send messages, the voice message is routed to the Unity Connection server for delivery.

When Unity Connection receives the voice message, it searches the list of SMTP proxy addresses for robin.smith@example.com (the sender) and chris.jones@example.com (the recipient). Because these addresses are defined as SMTP proxy addresses for the user profiles of Robin Smith and Chris Jones respectively, Unity Connection delivers the message as a voice message from Robin Smith to Chris Jones.

When Chris opens Outlook, the email message from Robin shows up as a new message in the Microsoft Exchange Inbox. The voice message from Robin, on the other hand, shows up as a new message in the Inbox of the Unity Connection account that Chris accesses via IMAP. If Chris replies to either message, the Outlook client will automatically route the reply by using the account in which Chris received the original message.

**Note** As Unity Connection is configured to be able to match the corporate email addresses in use at ExampleCo to Unity Connection user accounts (via the SMTP proxy address that is defined for each user), users can use the existing Outlook address book to address both email and voice messages. In addition, users do not need to think about which account to use to compose, reply to, or forward messages—this is all handled automatically by the Outlook and ViewMail configuration.

# Recommendations for Deploying IMAP Access in Cisco Unity Connection 10.x

When deploying IMAP clients to access and send Cisco Unity Connection messages, we recommend the following:

- Use a firewall to protect the Unity Connection SMTP port from unauthorized access. The SMTP port and domain are listed on the **System Settings > SMTP Configuration > Server** page in Cisco Unity Connection Administration.
- Configure Transport Layer Security for IMAP client connections in order to protect user passwords.
- Configure the corporate email address of each user as an SMTP proxy address for the user. When setting up the Unity Connection IMAP account on user workstations, use the corporate email address of the user, rather than the Unity Connection-specific email address, in the IMAP settings. In this way, users do not need to know an extra set of email addresses for addressing voice messages in the email client, and are insulated from changes to the Unity Connection-specific addresses if the Unity Connection SMTP domain is changed.
- ViewMail for Outlook limits the message recipients that a user can reach to objects that are in the search space of the user, and sends a non-delivery receipt (NDR) for messages that are sent to recipients that do not appear in the search space. If you are using search spaces to limit the objects that users can reach and do not want users to receive NDRs for unreachable objects, consider creating a separate Outlook address book for ViewMail users that is limited to the objects in the user search space.

# Task List for Configuring IMAP Access in Cisco Unity Connection 10.x

1. *If you plan to configure Cisco Unity Connection to relay messages for users to another SMTP server,* do the following subtasks:

   a. Configure the SMTP smart host to accept messages from the Unity Connection server. See the documentation for the SMTP server application that you are using.
   b. Configure the Unity Connection server to relay messages to the smart host. See the "Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host" section on page 23-5.
   c. Review the settings that control whether private or secure messages can be relayed. See the "Configuring Message Relay Settings" section on page 23-5.

2. Configure message actions for Unity Connection users or user templates. See the "Message Actions in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/0xcucmacx.html.
3. Configure SMTP proxy addresses for users who will send or receive messages from IMAP clients.See the "SMTP Proxy Addresses in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

**Note** At a minimum, we recommend that you configure the corporate email address of each user as an SMTP proxy address for the user.

4. Associate users with a class of service that offers a license to use an IMAP client to access voice messages. See the "IMAP Client Access to Voice Messages in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service Settings in Cisco Unity Connection 10.x " chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.
5. Configure SMTP proxy addresses for VPIM contacts who may receive messages from IMAP clients. See the "SMTP Proxy Addresses in Cisco Unity Connection 10.x" section in the "Managing Contacts in Cisco Unity Connection 10.x " chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.
6. Configure the Unity Connection server to allow SMTP connections from IMAP clients. See the "Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication" section on page 23-6.
7. *If you configured Transport Layer Security to be required or optional in the procedure in Task 6.*: Configure the Unity Connection server to provide a secure IMAP Unity Connection, as described in the "Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 10.x" section on page 28-2.
8. Optionally, modify the settings that determine the characteristics of SMTP messages that Unity Connection accepts. See the "Configuring SMTP Message Parameters" section on page 23-7.

9. For each user workstation, configure a supported IMAP client to access a Unity Connection mailbox.See the "Configuring an Email Account to Access Cisco Unity Connection 10.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_setup/guide/10xcucuwsx.html.

# Procedures for Configuring IMAP Access in Cisco Unity Connection 10.x

See the following sections:


- Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication, page 23-6
- Configuring Message Relay Settings, page 23-5
- Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication, page 23-6
- Configuring SMTP Message Parameters, page 23-7


## Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host

To enable Cisco Unity Connection to relay any type of message to the SMTP address for a user, your Unity Connection server must be configured to relay messages through a smart host.

### To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, expand **SMTP Configuration**, then select **Smart Host**.

**Step 2** On the **Smart Host** page, in the **Smart Host** field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

**Step 3** Select **Save**.

## Configuring Message Relay Settings

You can choose whether Cisco Unity Connection relays messages that are marked private or secure.

### To Configure Message Relay Settings

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, expand **Advanced**, then select **Messaging**.

**Step 2** To have Cisco Unity Connection relay messages that are marked private, check the **Allow Relaying of Private Messages** check box. (This check box is checked by default.) Unity Connection sets the private flag on the message when relaying a private message.

To prevent Unity Connection from relaying private messages, uncheck the check box. Unity Connection sends an NDR to the message sender when it receives a message that it cannot relay because the message is marked private.

**Step 3** To have Unity Connection relay secure messages, check the **Allow Relaying of Secure Messages** check box. (This check box is unchecked by default.) Unity Connection relays secure messages as regular messages.

To prevent Unity Connection from relaying secure messages, uncheck the check box. Unity Connection sends an NDR to the message sender when it receives a message that it cannot relay because the message is marked secure.

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

# Configuring the Cisco Unity Connection Server for IMAP Client Access and Authentication

You have a number of options for controlling which clients can initiate SMTP connections with Cisco Unity Connection. You can create an access list, which allows you to configure specific IP addresses or IP address patterns that correspond with clients that you wish to allow or deny access. You can also choose to allow all clients to connect, regardless of IP address; if you do so, you can specify whether those clients (known as untrusted IP addresses) must authenticate, and whether Transport Layer Security is required or allowed for clients with untrusted IP addresses.

If you choose to require clients with untrusted IP addresses to authenticate with Unity Connection, users enter their Unity Connection alias and Cisco PCApassword (also known as the web-application password) in the IMAP client to authenticate. Make sure that users understand that whenever they change their Cisco PCA password in the Unity Connection Messaging Assistant, they also must update the password in their IMAP client. If users have trouble receiving voice messages in an IMAP client after having updated their Cisco PCA password in both applications, see the "Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection 10.x" section in the "Configuring an Email Account to Access Cisco Unity Connection 10.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_setup/guide/10xcucuwsx.html .

Do one or both of the following procedures, as applicable.

- To Configure the Cisco Unity Connection IP Address Access List, page 23-6
- To Configure Access and Authentication for Untrusted IP Addresses, page 23-7

### To Configure the Cisco Unity Connection IP Address Access List

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Server**.

**Step 2** On the **SMTP Server Configuration** page, on the **Edit** menu, select **Search IP Address Access List**.

**Step 3** On the **Search IP Address Access List** page, select **Add New** to add a new IP address to the list.

**Step 4** On the **New Access IP Address** page, enter an IP address; or, you can enter a single * (asterisk) to match all possible IP addresses.

**Step 5** Select **Save**.

**Step 6** On the **Access IP Address** page, to allow connections from the IP address that you entered in Step 4, check the **Allow Unity Connection** check box. To reject connections from this IP address, uncheck the check box.

**Step 7** If you have made any changes on the **Access IP Address** page, select **Save**.

**Step 8** Repeat Step 2 through Step 7 for each additional IP address that you want to add to the access list.

#### To Configure Access and Authentication for Untrusted IP Addresses

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Server**.

**Step 2** On the **SMTP Server Configuration** page, check the **Allow Connections From Untrusted IP Addresses** check box to allow all clients to connect by using SMTP, regardless of whether Unity Connection is configured to specifically allow connections from their IP addresses.

**Step 3** If you checked the check box in Step 2, check the **Require Authentication From Untrusted IP Addresses** check box to configure authentication for these types of clients. Then, select how Unity Connection handles Transport Layer Security for untrusted IP addresses:

- Disabled—Unity Connection does not offer TLS as an option for SMTP sessions that are initiated by clients or servers with untrusted IP addresses. In most cases, if the client is configured to use TLS, but Unity Connection does not offer it, the Unity Connection fails and the client notifies the user.
- Required—Clients or servers connecting from untrusted IP addresses must use TLS to initiate SMTP sessions with the Unity Connection server.
- Optional—Clients or servers connecting from untrusted IP addresses can use TLS to initiate SMTP sessions with the Unity Connection server, but are not required to do so.

**Note** To protect user passwords, we recommend that you require authentication from untrusted IP addresses and configure Transport Layer Security as either Required or Optional.

**Step 4** If you chose Required or Optional for the Transport Layer Security setting in Step 3, to configure TLS on the Unity Connection server, see the "Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 10.x" section on page 28-2.

# Configuring SMTP Message Parameters

You can configure Unity Connection to reject any incoming SMTP messages that are larger than a configurable total size or have more than a configurable number of recipients. By default, Unity Connection accepts messages that are larger than 10 MB or have more than 15,000 recipients.

### To Configure SMTP Message Parameters

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Server**.

**Step 2** On the **SMTP Server Configuration** page, in the **Limit Size of Message** field, enter a number in kilobytes to limit the size of an individual message sent by an SMTP client.

**Step 3** In the **Limit Number of Recipients per Message** field, enter the number of recipients allowed per message.

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

# Configuring Transcription (SpeechView) in Cisco Unity Connection 10.x

**Note** This chapter contains information on setting up Cisco Unity Connection so that users can view transcriptions of their voice messages.

See the following sections:


- Overview of SpeechView in Cisco Unity Connection 10.x, page 24-1
- SpeechView Security Considerations, page 24-3
- Recommendations for Deploying SpeechView, page 24-3
- Task List for Configuring SpeechView in Cisco Unity Connection 10.x, page 24-4
- Procedures for Configuring SpeechView in Cisco Unity Connection 10.x, page 24-5
- SpeechView Reports in Cisco Unity Connection 10.x, page 24-8


## Overview of SpeechView in Cisco Unity Connection 10.x

SpeechView feature allows you to receive voice messages in your mail box in the form of text. When a voice message arrives, it is delivered to the mailbox of the recipient with a blank text attachment. When the completed transcription is returned by the transcription service, the text attachment is updated with the text of the transcription, or with an error message if there was a problem with the transcription. Only the first 500 characters of a message transcription are provided, so longer messages are truncated. However, users have access to the original recording in its entirety.

SpeechView is a feature of the Unity Connection unified messaging solution, therefore, the original audio version of each voice message remains available to you anywhere, anytime.

**Note** When a voice message is sent from Web Inbox to VMO, the voice message is delivered to the mailbox of the recipient along with the transcribed text in the both in the transcript view box and in the mail body.

When the SpeechView feature is enabled, Cisco Unity Connection uses a third-party external transcription service to convert voice messages to text. The SpeechView feature provides the following types of transcription services:

- **Standard Transcription Service:** Works as a fully automated non human assisted transcription service. In the standard transcription service, the transcription service automatically converts the voice message to text and then the transcription received from Unity Connection is sent to the recipient through e-mail.
- **Professional Transcription Service:** Involves automated transcription and human intervention, if required, to convert voice messages to text. In the professional transcription service, the transcription service first converts the voice message to text automatically and confirms the accuracy of the transcription. If the accuracy is low in any part of transcription, the particular part of transcription is sent to a human operator who reviews the audio and improves the quality of the transcription. As the professional transcription service involves both automatic transcription and human intervention, the accuracy of text message is more as compared to the standard transcription service. The professional transcription service is also known as SpeechView Pro service.

**Note** Unity Connection supports only standard transcription service that involves automatic conversion of voice message to text without any human intervention.

Unity Connection sends the audio portion of a voice message to the transcription service, without details about the sender or recipients of the message. Communication between Unity Connection and the external transcription service is secured by using S/MIME over SMTP.

To use SpeechView, users must belong to a class of service that enables transcriptions of voice messages. The class of service specifies the type of transcription service, either Standard or Professional, for which the user is subscribed. Members of the class of service can view the transcriptions of their messages by using an IMAP client that is configured to access their Unity Connection messages. The original voice message remains attached to the transcribed text message.

For more information on enabling class of service, see the "SpeechView Transcriptions of Voice Messages in Cisco Unity Connection 10.x" section of the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

You can also configure an SMS or SMTP notification device for users so that Unity Connection sends transcriptions to an SMS-compatible phone or an external email address; users can configure SMS or SMTP notification devices for themselves if they have access to the Unity Connection Messaging Assistant web tool. The original voice message is not attached to transcription messages sent to notification devices, but the device can be configured to include the phone number that users call to reach Unity Connection, so after viewing the transcription they can call Unity Connection to listen to the voice message.

The following messages are never transcribed:

- Private messages
- Broadcast messages
- Dispatch messages
- Secure messages (configurable)
- Messages with no recipients in an enabled class of service

**Note** Messages with no recipients in an enabled COS includes those messages that are sent to a group of recipients and no recipient from the group is subscribed for the SpeechView transcription service. In such cases, the voice message is not transcribed for any of the recipients.

Secure messages are transcribed only if the user belongs to a class of service for which the Allow Transcriptions of Secure Messages option is enabled.

**Note** Unity Connection supports only the UTF-8 character set encoding for transcription.

# SpeechView Security Considerations

All transcriptions are handled by a third party transcription service outside of the customer environment. Communication between the customer Cisco Unity Connection server and the transcription service is handled through the use of S/MIME. The S/MIME public and private key negotiation happens transparently when registering with the transcription service. A new key pair is created each time a system registers.

When messages are sent to the transcription service, customer information is not passed with the message. The transcription service is unaware of the specific user the message belongs to. If human involvement is required in the transcription, the person working on the transcription is not able to determine the user or company from which the message originated. All audio stays on the conversion system and is never stored on the workstation of the person who processes the transcription. After the transcribed message is sent to the Unity Connection server, the copy at the transcription service is purged.

# Recommendations for Deploying SpeechView

### Advantages to Forwarding Personal Phones to Unity Connection

To take full advantage of SpeechView, encourage users to configure their mobile phones to forward to Unity Connection so that all of their voice messages are available in one mailbox and are all transcribed. To do this, users would configure the mobile phone to forward to their work phone number, which should correspond to their primary extension on Unity Connection. To configure the mobile phone for call forwarding, obtain specific instructions from the mobile phone carrier. A generic procedure is provided in the "Task List for Consolidating Your Voicemail from Multiple Phones into One Mailbox" section of the "Changing Your User Preferences" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html. Note that due to the call going to the mobile phone first and then to the work phone, callers may hear a lot of rings before reaching the mailbox of the user. To avoid this problem, you can instead forward the mobile phone to a special DID number that does not ring a phone and forwards directly to the mailbox of the user. This can be accomplished by adding the DID number as an alternate extension for the user.

### Using SpeechView with Networked Cisco Unity Connection Servers

To consolidate the interface between the customer and the third-party transcription service, configure one of your Cisco Unity Connection servers (or clusters) to act as a proxy for the other Unity Connection servers in the network. In this configuration, only the proxy server registers with the transcription service. This can make it easier to troubleshoot any problems with transcriptions, track your transcription usage and monitor the load it introduces to your network.

If one of your Unity Connection servers has a lower call volume than others in the network, consider designating it as the proxy server for transcriptions.

If you do not use a proxy server for transcriptions, you need a separate external-facing SMTP address for each server (or cluster) in the network.

See the "Task List for Configuring SpeechView in Cisco Unity Connection 10.x" section on page 24-4 for detailed instructions.

### Using SpeechView with Relay or Accept and Relay Message Actions

If user accounts are configured to relay voice messages to an alternate SMTP address, their voice messages cannot be transcribed. If users want transcriptions as well as the relay feature, you can instead configure user accounts to accept and relay voice messages. This allows the copy of the message that is stored on the Unity Connection server to be transcribed. Configure SMTP notification devices for users so that the transcription is sent to their SMTP address. This means that users will receive two emails at their SMTP address. The first one is the relayed copy of the message WAV file. The second is the notification that includes the transcription. If users do not want two emails for each message, consider setting their account to accept messages so that they receive only the email with the transcription. If they need to access the original recording, users can call to Unity Connection or use an IMAP client to access their Unity Connection account.

For more information on message actions such as relay and accept and relay, see the "Message Actions in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Task List for Configuring SpeechView in Cisco Unity Connection 10.x

1. *Confirm that you have installed a license file that enables the SpeechView feature. For more information on managing and installing license file, see* Managing Licenses in Cisco Unity Connection 10.x.
2. Associate users with a class of service that provides SpeechView transcriptions of voice messages. See the "SpeechView Transcriptions of Voice Messages in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by Class of Service in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.
3. Configure an SMTP smart host to accept messages from the Unity Connection server. See the documentation for the SMTP server application that you are using.
4. Configure the Unity Connection server to relay messages to the smart host. See the "Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host" section on page 24-5.
5. *(When Unity Connection is configured to refuse connections from untrusted IP addresses)* Configure the Unity Connection server to receive messages from your email system. See the "Configuring the Cisco Unity Connection Server to Accept Messages From Your Email System" section on page 24-5.
6. Configure your email infrastructure system to route incoming SpeechView traffic to the Cisco Unity Connection server. See the "Configuring Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server" section on page 24-6.

7. Configure the SpeechView transcription service. See the "Configuring the SpeechView Transcription Service" section on page 24-7.
8. Configure SMS or SMTP notification devices for Unity Connection users or user templates. See the "Transcription Delivery with SpeechView in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Procedures for Configuring SpeechView in Cisco Unity Connection 10.x

See the following sections:


- Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host, page 24-5
- Configuring the Cisco Unity Connection Server to Accept Messages From Your Email System, page 24-5
- Configuring Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server, page 24-6
- Configuring the SpeechView Transcription Service, page 24-7


## Configuring the Cisco Unity Connection Server to Relay Messages to a Smart Host

To enable Cisco Unity Connection to send messages to the external transcription service, you must configure the Unity Connection server to relay messages through a smart host.

### To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Smart Host**.

**Step 2** On the **Smart Host** page, in the **Smart Host f**ield, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

**Step 3** Select **Save**.

## Configuring the Cisco Unity Connection Server to Accept Messages From Your Email System

Do the following procedure.

#### To Configure the Cisco Unity Connection Server to Accept Messages From Your Email System

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Server**.

**Step 2** On the **SMTP Server Configuration** page, on the **Edit** menu, select **Search IP Address Access List**.

**Step 3** On the **Search IP Address Access List** page, select **Add New** to add a new IP address to the list.

**Step 4** On the **New Access IP Address** page, enter the IP address of your email server.

**Step 5** Select **Save**.

**Step 6** To allow connections from the IP address that you entered in Step 4, on the **Access IP Address** page, check the **Allow Unity Connection** check box.

**Step 7** If you have made any changes on the **Access IP Address** page, select **Save**.

**Step 8** If you have more than one email server in your organization, repeat Step 2 through Step 7 to add each additional IP address to the access list.

# Configuring Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server

Do the following procedure.

#### To Configure Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server

**Step 1** Select an external-facing SMTP address that the third party transcription service will use to send transcriptions to the Cisco Unity Connection server. For example, select "transcriptions@<yourdomain.com>"

If you have more than one Unity Connection server, you need a separate external-facing SMTP address for each server, unless the servers are part of a Unity Connection cluster. Alternatively, you can configure one Unity Connection server or cluster to act as a proxy for the remaining servers or clusters in the digital network.

**Step 2** For each external-facing SMTP Address that you selected in Step 1, configure your email infrastructure to route messages that are sent the SMTP address to the "stt-service" alias on the Unity Connection server. For example, if the SMTP domain for the Unity Connection server is "Unity Connectionserver1.cisco.com," the email infrastructure must be configured to route "transcriptions@cisco.com" to "stt-service@connectionserver1.cisco.com."

If you are configuring SpeechView on a Unity Connection cluster, configure the smart host to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for incoming transcriptions to reach the cluster subscriber server in the event that the publisher server is down.

**Step 3** Add "nuancevm.com" to the "safe senders" list in the email infrastructure so that incoming transcriptions do not get filtered out as spam.

**Note** In Cisco Unity Connection, to avoid timeout or failure of the registration request with the Nuance server, make sure to:

- Remove the email disclaimers from the inbound and outbound email messages between Unity Connection and the Nuance server.

- Maintain SpeechView registration messages in the S/MIME format.

# Configuring the SpeechView Transcription Service

Do the following procedure.

**To Configure the SpeechView Transcription Service**

**Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging > SpeechView Transcription Service**.

In Cisco Unity Connection Administration, expand **System Settings > External Services**, and then select **Transcription for SpeechView**.

**Step 2** On the **SpeechView Transcription Service** page, check the **Enabled** check box.

**Step 3** If this server will access transcription services through another Unity Connection location that is digitally networked, do the following sub-steps:

**a.** Select **Access Transcription Services Through** Unity Connection **Proxy Location**.

**b.** Select the name of the Unity Connection location from the list.

**c.** Select **Save**.

**d.** Skip to Step 9.

Otherwise, if this server is going to access transcription services directly, select **Access Transcription Service Directly**.

**Step 4** In the **Incoming SMTP Address** field, enter the email address that will be recognized by your email infrastructure and routed to the "stt-service" alias on the Unity Connection server. (This is the email address that you chose in Step 1 of the "To Configure Your Email System to Route Incoming SpeechView Traffic to the Cisco Unity Connection Server" procedure on page 24-6.

**Step 5** In the **Registration Name** field, enter a name that will uniquely identify the Unity Connection server within your organization. This name is used by the third-party transcription service to identify this server for registration and subsequent transcription requests.

**Step 6** If you want this server to offer transcription proxy services to other Unity Connection locations in a digital network, check the **Advertise Transcription Proxy Services to Other** Unity Connection **Locations** check box.

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

**Step 8** Select **Register**.

Another window displaying the results will open. The registration process normally takes several minutes. Wait for the registration process to complete successfully before going on to the next step.

If registration does not complete within 5 minutes, there may be a configuration issue. The registration process will timeout after 30 minutes.

**Step 9** Select **Test**.

Another window displaying the results will open. The test will usually take several minutes, but can take up to 30 minutes.

# SpeechView Reports in Cisco Unity Connection 10.x

Cisco Unity Connection can generate the following reports about SpeechView usage:

- **SpeechView Activity Report by User** —Shows the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user.
- **SpeechView Activity Summary Report**—Shows the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. Note that when messages are sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once.

For details on generating reports, see the "Reports in Cisco Unity Connection 10.x" chapter.

# Managing Mailbox Stores in Cisco Unity Connection 10.x

See the following sections:


- How Multiple Mailbox Stores Work in Cisco Unity Connection 10.x, page 25-1
- Creating a Mailbox Store in Cisco Unity Connection 10.x, page 25-4
- Moving Mailboxes Between Mailbox Stores in Cisco Unity Connection 10.x, page 25-5
- Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged in Cisco Unity Connection 10.x, page 25-6
- Deleting a Mailbox Store in Cisco Unity Connection 10.x, page 25-6
- Disabling and Re-Enabling a Mailbox Store in Cisco Unity Connection 10.x, page 25-7


## How Multiple Mailbox Stores Work in Cisco Unity Connection 10.x

During installation, Cisco Unity Connection automatically creates:

- A directory database for system configuration information (user data, templates, classes of service, and so on).
- A mailbox store database for information on voice messages (who each message was sent to, when it was sent, the location of the WAV file on the hard disk, and so on).
- An operating-system directory for voice message WAV files.

An administrator with the required permissions can create up to four additional mailbox stores. Each additional mailbox store includes:

- Another mailbox-store database for information on voice messages that are saved in that mailbox store. The database is presized for an average of approximately 40 messages each for 10,000 users, or about 1.25 GB. (The database application currently being used for Unity Connection cannot dynamically resize a database after it is created.)
- Another operating-system directory for the voice message WAV files and other message attachments saved in that mailbox store.

Although there is one mailbox-store database for each mailbox store, there is only one directory database for the entire system. If you create an additional mailbox store and move the mailboxes for selected users to the new store, the directory information for the users remains in the directory database that was created when Unity Connection was installed.

Creating additional mailbox stores is primarily useful for ensuring that backups will complete during non-business hours. For more information, see the "Backups with Multiple Mailbox Stores" section on page 25-3.

After you create a new mailbox store, you can either move existing mailboxes into the new store or you can create new mailboxes in the new store. For information on moving existing mailboxes into the new store, see the "Moving Mailboxes Between Mailbox Stores in Cisco Unity Connection 10.x" section on page 25-5.

See the following sections for additional details:

- Replication, page 25-2
- User Templates, page 25-2
- Maximum Size of a Mailbox Store Before Warnings Are Logged, page 25-3
- Backups with Multiple Mailbox Stores, page 25-3

# Replication

When you install two or more Cisco Unity Connection servers in a cluster, all mailbox stores are replicated to all servers in the cluster.

# User Templates

When you create a new user account, you select the template whose settings are used as the default values for the new user account. One of the template settings specifies the mailbox store in which the mailbox is created. All default templates specify that mailboxes be created in the default mailbox store. If you create new mailbox stores, you can change this setting in the default templates and in any new templates that you create.

When you create a new template or edit a template to change the mailbox store in which new mailboxes are created, Cisco Unity Connection Administration allows you to select a mailbox store that is currently disabled. However, when you create a user account by using the template, if the store is still disabled, creating the user account fails.

If a mailbox store is the default mailbox store for one or more templates, you cannot delete that mailbox store until the template setting is changed or the template is deleted.

For more information on templates, see the "Adding, Modifying, or Deleting a User Template in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Maximum Size of a Mailbox Store Before Warnings Are Logged

When you create a new mailbox store, you specify the maximum amount of disk space that the voice messages for the mailbox store can occupy. The maximum size is not an absolute maximum. When a mailbox store reaches the specified value:

- Unity Connection still saves new messages in the mailbox store.
- You can still create new mailboxes in the mailbox store.
- You can still move mailboxes into the mailbox store.

When the size of the store reaches 90 percent of the specified maximum size, a warning is logged in the system log.

When the size of the store reaches 100 percent of the specified maximum size, an error is logged in the system log. In addition, in Cisco Unity Connection Administration, an error appears in the **Status** bar on the **Edit Mailbox Store** page.

If you want to keep the mailbox store under 100 percent of the specified maximum size, you can:

- Increase the maximum size of the mailbox store, if there is additional space available on the hard disk. See the "Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged in Cisco Unity Connection 10.x" section on page 25-6. Do not use this option if the mailbox store is already at the maximum size that can be backed up during non-business hours.
- Have users delete messages to reduce the size of their mailboxes, which also reduces the total size of the mailbox store.

**Note** When users delete messages, the deleted messages are not removed from the mailbox store until the next time that the Clean Deleted Messages task runs. This task runs every 30 minutes; the schedule cannot be edited.

- Revise the message aging policy or mailbox size quotas to reduce the size of individual mailboxes and, therefore, the size of the mailbox store. We recommend that you have users delete messages from their mailboxes first, so that users who are not currently over the quota are not forced over the quota by the new values. For more information on message aging policy and on mailbox size quotas, see the "Controlling the Size of Mailboxes in Cisco Unity Connection 10.x" chapter.
- Create another mailbox store and move some mailboxes into the new mailbox store.

# Backups with Multiple Mailbox Stores

When deciding on the maximum size for a mailbox store, consider the duration of backups. The Disaster Recovery System must back up an entire mailbox store and the corresponding database during a single backup session. Because the Disaster Recovery System has a significant impact on system performance, each mailbox store must be a size that can be backed up during non-business hours. We chose the default size of 15 GB (approximately 30 minutes of recordings for each of 1,000 users when the codec is G.711)

because a mailbox store of that size can be backed up in about six hours at 3 GB per hour. (The maximum size of a mailbox store does not include the 1.25 GB for the database that contains information on the messages in the mailbox store.)

**Caution** For tape backups, the Disaster Recovery System can only save one backup session on a tape. If you create multiple mailbox stores and back up the stores in separate sessions, you must change tapes between sessions or the second backup overwrites the first backup.

For more information on how to back up multiple mailbox stores, see the applicable document for Cisco Unity Connection, see the *Disaster Recovery System Administration Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/drs_administration/guide/10xcucdrsag.html.

# Creating a Mailbox Store in Cisco Unity Connection 10.x

### To Create a Mailbox Store

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the **System Administrator** role.

**Note** A user account that does not have the **System Administrator** role cannot create a new mailbox store.

**Step 2** Expand **Message Storage**, then select **Mailbox Stores**.

**Step 3** On the **Search Mailbox Store** page, select **Add New**.

**Step 4** On the **New Mailbox Store** page, enter settings as applicable.

**Note** Fields marked with an * (asterisk) are required.

**Step 5** Select **Save**.

**Note** Creating the database for the new mailbox store requires several minutes.

When the new mailbox store has been created, it appears in the table on the **Search Mailbox Stores** page, the value of the **Access Enabled** column changes to **Yes**, and the value of the **Status** column changes from **Creating Mailbox Store** to **OK**.

**Note** It is recommended to configure a maximum of 5000 user mailboxes in a single mailstore for optimal performance.

# Moving Mailboxes Between Mailbox Stores in Cisco Unity Connection 10.x

When moving mailboxes between mailbox stores, note the following:

- When a mailbox is moved to another message store, the MWI status is retained.
- When clustering is configured, you must sign in to the server whose server status is primary to move mailboxes.
- Moving a mailbox fails if:
  - The administrator currently signed in to Cisco Unity Connection Administration is not authorized to move a mailbox.
  - The source or target mailbox store is disabled because, for example, the mailbox store is being backed up.
  - The mailbox is disabled.
  - The user whose mailbox you are moving is a system user. System mailboxes cannot be moved out of the default mailbox store, UnityMbxDb1.

### To Move Mailboxes from One Mailbox Store to Another

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

**Note** A user account that does not have the System Administrator role cannot move mailboxes between mailbox stores.

**Step 2** In Cisco Unity Connection Administration, expand **Message Storage**, then select **Mailbox Stores Membership**.

**Step 3** On the **Search Mailbox Stores Membership** page, in the **Choose Membership Type** list, select **User Mailbox**.

**Step 4** Under **User Mailbox Search Results**, specify the mailbox store from which you want to move mailboxes.

**Step 5** Specify search criteria to further identify the users whose mailboxes you want to move, and select **Find**.

The specified users appear in the table at the bottom of the page.

**Step 6** Select the mailbox store to which you want to move mailboxes.

**Step 7** Check the applicable check boxes to select the users whose mailboxes you want to move.

**Step 8** Select **Move Selected Mailboxes**.

# Changing the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged in Cisco Unity Connection 10.x

### To Change the Maximum Size a Mailbox Store Can Reach Before Warnings Are Logged

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the **System Administrator** role.

**Note** A user account that does not have the **System Administrator** role cannot change the size of a mailbox store.

**Step 2** In Cisco Unity Connection Administration, expand **Message Storage**, then select **Mailbox Stores**.

**Step 3** On the **Search Mailbox Store** page, select the name of the mailbox store.

**Step 4** On the **Edit Mailbox Store** page, change the value of the **Maximum Size Before Warning** field.

**Step 5** Select **Save**.

# Deleting a Mailbox Store in Cisco Unity Connection 10.x

Cisco Unity Connection Administration does not allow an administrator to delete a mailbox store when any of the following are true:

- The mailbox store still contains one or more mailboxes.
- The mailbox store is still referenced by one or more templates.
- The administrator who is trying to delete the mailbox store does not have permission to delete a mailbox store.
- The administrator is trying to delete the default mailbox store, UnityMbxDb1.

### To Delete a Mailbox Store

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the **System Administrator** role.

**Note** A user account that does not have the **System Administrator** role cannot delete a mailbox store.

**Step 2** If you know the mailbox store does not contain any mailboxes, skip to Step 3. If you do not know, do the following steps to find mailboxes, if any, and to move them to other mailbox stores:

a. In Cisco Unity Connection Administration, expand **Message Storage**, then select **Mailbox Stores Membership**.

b. In the **Choose Membership Type** list, select **User Mailbox**.

c. Under **User Mailbox Search Results**, specify the mailbox store from which you want to move mailboxes.

d. Specify search criteria to further identify the users whose mailboxes you want to move, and select **Find**.

The specified users appear in the table at the bottom of the page.

e. Select the mailbox store to which you want to move mailboxes.

f. Check the applicable check boxes to select the users whose mailboxes you want to move.

g. Select **Move Selected Mailboxes**.

**Step 3** If you know that no user templates reference the mailbox store that you want to delete, skip to Step 4. If you do not know, do the following steps to find templates, if any, and to reassign the templates to other mailbox stores:

a. On the **Search Mailbox Stores Membership** page, in the **Choose Membership Type** list, select **User Template**.

b. Under **User Mailbox Search Results**, select the options to find the user templates that reference the mailbox store that you want to delete, and select **Find**.

c. If any templates are found, check the applicable check boxes to select them, select the mailbox store that you want the templates to reference instead, and select **Assign Selected Templates**.

**Step 4** In Cisco Unity Connection Administration, expand **Message Storage**, then select **Mailbox Stores**.

**Step 5** On the **Search Mailbox Store** page, check the check box for the mailbox store that you want to delete.

**Step 6** Select **Delete Selected**.

**Step 7** Select **OK** to confirm.

# Disabling and Re-Enabling a Mailbox Store in Cisco Unity Connection 10.x

Each mailbox store is disabled automatically while it is being backed up by the Disaster Recovery System. When a mailbox store is disabled:

- You cannot create a new mailbox in the store.
- You cannot move existing mailboxes into or out of the store.
- New messages for users whose mailboxes are in the disabled store are queued for delivery when the store is re-enabled.

Although Cisco Unity Connection Administration includes an option to manually disable a mailbox store, there is currently no reason to do so.

# Controlling the Size of Mailboxes in Cisco Unity Connection 10.x

**Note** To help control the size of user voice mailboxes, you can use Cisco Unity Connection Administration to specify mailbox size quotas and to change the message aging policy. See the following sections:


- Specifying Mailbox Size Quotas in Cisco Unity Connection 10.x, page 26-1
- Managing Mailbox Quota Alert in Cisco Unity Connection 10.x, page 26-3
- Managing Message Aging Policies in Cisco Unity Connection 10.x, page 26-4
- Message Recording Expiration, page 26-9


## Specifying Mailbox Size Quotas in Cisco Unity Connection 10.x

To help control the size of user voice mailboxes, Cisco Unity Connection lets you specify quotas, or limits, on the maximum size of voice mailboxes. By default, Unity Connection is configured with the systemwide mailbox size quotas listed in Table 26-1. To change systemwide quotas, do the "To Change the Default Systemwide Quotas" procedure on page 26-2.

**Caution** Quotas are not enforced for messages left by outside callers if the "Full Mailbox Check for Outside Caller Messages" check box is not checked. This check box appears on the Message Storage > Mailbox Quotas page. For more information, see Help for that page.

You can override systemwide quotas by specifying custom quotas for users and for templates. For a procedure, see the "Mailbox-Size Quotas in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

**Caution** Quotas alone are only practical for controlling the size of mailboxes for users who regularly check Unity Connection voice messages by using the telephone user interface. Web Inbox and ViewMail for Outlook do not inform users that their mailbox has reached its quota. If users check messages primarily or

exclusively by using Web Inbox or ViewMail for Outlook, configure message aging, too, so old messages are automatically deleted. See the "Managing Message Aging Policies in Cisco Unity Connection 10.x" section on page 26-4.

When single inbox is configured, messages that users delete by using Outlook are only moved to the Deleted Items folder in Outlook, not permanently deleted. When Unity Connection synchronizes with Exchange, messages that have been deleted in Outlook are moved to the Unity Connection Deleted Items folder; the messages are not permanently deleted from Unity Connection. If you configure message quotas in this configuration, we recommend that you also configure message aging. For more information on message aging, see the "Managing Message Aging Policies in Cisco Unity Connection 10.x" section on page 26-4.

*Table 26-1 Mailbox-Size Quotas by Codec*

| Quota Level | Mailbox Size That Triggers Quota Action | Action When Quota Is Reached | Recording Time Before Quota Is Reached/ Disk Space Used | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | G.711 Mu-Law | G.711 A-Law | G.726 | PCM 8 kHz | G.729a | GSM 6.10 |
| Warning | 12 MB | The user is warned that the mailbox is reaching the maximum size allowed. | 18 min./ 11 KB/sec | 18 min./ 11 KB/sec | 37 min./ 5.53 KB/sec | 9 min./ 22 KB/sec | 122 min./ 1.67 KB/sec | 91 min./ 2.25 KB/sec |
| Send | 13 MB | The user is prevented from sending any more voice messages. | 20 min./ 11 KB/sec | 20 min./ 11 KB/sec | 40 min./ 5.53 KB/sec | 10 min./ 22 KB/sec | 132 min./ 1.67 KB/sec | 98 min./ 2.25 KB/sec |
| Send/ Receive | 14 MB | The user is prevented from sending or receiving any more voice messages. | 21 min./ 11 KB/sec | 21 min./ 11 KB/sec | 43 min./ 5.53 KB/sec | 10 min./ 22 KB/sec | 143 min./ 1.67 KB/sec | 106 min./ 2.25 KB/sec |

### To Change the Default Systemwide Quotas

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then select **Mailbox Quotas**.

**Step 2** Set values for the following quotas, as applicable, by selecting **Custom** and then entering a value (in megabytes) in the adjacent field:

- Warning Quota
- Send Quota
- Send/Receive Quota

**Note** The value for **Warning Quota** must be smaller than or equal to the value for **Send Quota,** and that the value for **Send Quota** must be smaller than or equal to the value for **Send/Receive Quota.**

**Step 3** If you want Unity Connection to determine whether a user mailbox is full before allowing an outside caller to leave a message for the user, check the **Full Mailbox Check for Outside Caller Messages** check box.

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

# Managing Mailbox Quota Alert in Cisco Unity Connection 10.x

Cisco Unity Connection allows you to specify the maximum size or quota for the voice mailbox of every user in a Unity Connection system. In Unity Connection 9.1(1) and earlier releases, when a user exceeds the maximum assigned quota, the user is prompted within the Telephone User Interface for the voice mailbox quota overflow.

Beginning with Cisco Unity Connection 10.0(1) and later releases, when the voice mailbox size of a user starts reaching its specified threshold limit on Unity Connection, the user will receive a quota notification message.

A quota notification message is an email that is sent automatically by Unity Connection to the corporate email address of the voice mailbox when the voice mailbox size of the user exceeds it's threshold limit. You can use Cisco Unity Connection Administration to view the default quota notification message or to create, view, and modify customized quota notification messages.

The quota notification message is sent by the **Quota Notification Mail** task to the configured corporate addresses of the users whose voice mailbox has reached the size specified for warning quota. By default, the task is scheduled to run at 11:00 P.M. on daily basis. However, you can also customize the time and the interval after which the task must run. For more information on scheduling a task, refer to the "Task Schedule" section of "Cisco Unity Connection 10.x Tool Settings" chapter of *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

**Note** The quota notification messages are not sent to the users whose corporate email addresses are not configured.

You can also execute the following command through CLI to run the **Quota Notification Mail** task:

```
run cuc sysagent task Umss.QuotaNotificationMailTask
```

Where **Umss.QuotaNotificationMailTask** is the name of the **Quota Notification Mail** task.

For more information on this command, see the "run cuc sysagent task" section of the "Run commands" chapter of *Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 10.0(1)* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cli_ref/10_0_1/CUCM_BK_CBEED39F_00_cucm-cli-reference-guide-100_chapter_0101.html.

# Configuring Mailbox Quota Alert Text

If you want to customize the Subject Line or Body Text of the mailbox quota alert emails that are sent to users, do the following procedure.

### To Customize the Mailbox Quota Alert Text

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage> Mailbox Quotas** and then select **Quota Alert Text**.

**Step 2** On the **Edit Mailbox Quota Alert Text** page, in the **Language** list, select the applicable language.

**Step 3** To customize text for a mailbox **Quota Alert Text,** do the following sub-steps:

a. Uncheck the **Use Default Text** check box.

b. Enter text in the **Subject Line** and **Body Text** fields bases on your requirements . See Table 24-1 for a list of available parameters.

**Step 4** Select Save.

**Step 5** Repeat Step 2 through Step 4 for each language installed on the system.

*Table 26-2 Mailbox Quota Alert Text Parameters*

| Parameter | Description |
|---|---|
| %CURRENTUSAGE% | When the %CURRENTUSAGE % parameter is used, it is replaced with the current voice mailbox size of the user. |
| %THRESHOLD% | When the % THRESHOLD% parameter is used, it is replaced with the warning quota size specified by the administrator. |
| %LIMIT% | When the %LIMIT % parameter is used, it is replaced with the maximum size allowed for voice mailbox or Send/Receive Quota. |

# Managing Message Aging Policies in Cisco Unity Connection 10.x

Message aging policies can help ensure that the hard disk where voice messages are stored does not fill up. Each policy allows you to specify message aging rules to automatically:

- Move new messages to the Saved Items folder after a specified number of days.

  This option is primarily useful for users whose message action is **Accept and Relay the Message**, which causes Unity Connection to relay copies of voice messages to an external mail account while also saving the messages to the Unity Connection message store. You can use this option to prevent users who only check voice messages by using the external mail account from exceeding their mailbox quota.

  For more information, see the "Message Actions in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

- Move read messages to the Deleted Items folder after a specified number of days.

- Permanently delete messages in the Deleted Items folder after a specified number of days. In the Default System Policy message aging policy, this is the only rule that is enabled.
- Based on the age of the messages, permanently delete secure messages that have been touched in any way (for example by saving, deleting, or opening but then saving messages as new).
- Based on the age of the messages, permanently delete all secure messages regardless of whether users have listened to or touched the messages in any way.

If you only need one set of message aging rules, you can change the specifications for the default message aging policy and assign that one policy to all users and all templates. If you need to allow some users to retain messages longer than other users, you can create additional policies and assign different policies to user templates and to individual users. If you want to send message aging alerts to some users and not to others, you can create additional policies that include aging alerts.

For each policy, you can enable or disable each message aging rule, and you can specify a different number of days for each rule. For each message aging rule, you can also specify whether Unity Connection sends an email alert to users prior to aging the message.

You can also enable or disable an entire message aging policy; disabling a policy means that the rules in that policy are not enforced regardless of their settings. Unity Connection includes a default policy, **Do Not Age Messages**, that is disabled and for which all of the rules are disabled.

Some of the message aging rules are based on when a message was last modified. To modify a message, a user must do one of the following:

- In the Unity Connection Web Inbox or Messaging Inbox , mark the message as new, mark the message as deleted, or change the message subject, and select Save.
- From the phone interface, select the option to mark the message as new, resave the message, delete the message, or restore a deleted message as saved.

Simply listening to the message, without choosing one of these options, does not change the modification time of the message.

**Note** The schedule for message aging is controlled by the message aging task under **Task Management** in Cisco Unity Connection Administration.

See the following sections for additional details:

- About Message Aging Alerts, page 26-6
- Adding a Message Aging Policy, page 26-6
- Changing a Message Aging Policy, page 26-7
- Deleting a Message Aging Policy, page 26-7
- Configuring a Smart Host for Message Aging Alerts, page 26-8
- Configuring Message Aging Alert Text, page 26-8
- “Configuring Message Aging When Single Inbox Is Configured” section on page 26-9
- The “Message Aging in Cisco Unity Connection 10.x” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# About Message Aging Alerts

For each message aging rule, you can specify whether Unity Connection sends email alerts to users prior to taking the aging action that is associated with the rule. This gives users time to review and act on the applicable messages. You specify the number of days between the time that Unity Connection sends the alert and the time that the message aging action takes place.

Alerts cannot be sent to users unless the Corporate Email Address field for each user on the **Users > Users > Edit User Basics** page contains a valid email address. Unity Connection must also be configured to relay messages through an SMTP smart host.

You can customize the text in the email alerts or you can use the default text. The default subject line and body text are different for the alerts related to each aging rule, and they can be customized separately.

**Note** As all message aging policies use the same five rules, if you customize the alert text for a rule, the text will be the same for any policy that uses that rule. (For example, if you customize the email subject line and body text for the **Move Saved Messages to the Deleted Items Folder** rule, that text is used for all alerts that are sent to users who are assigned to any message aging policy for which that rule is enabled with alerts.)

Message aging alerts can be customized for multiple languages.

# Adding a Message Aging Policy

Cisco Unity Connection includes a **Default System Policy** and a **Do Not Age Messages** policy, which is the policy that you assign to users whose messages should never be automatically deleted. If you want more than these two policies, do the following procedure.

### To Add a Message Aging Policy

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then expand **Message Aging**, then select **Aging Policies**.

In Cisco Unity Connection Administration, expand **Message Storage**, then select **Message Aging Policy**.

**Step 2** Select **Add New**.

**Step 3** Enter a name for the new policy, and select **Save**.

**Step 4** Check the **Enabled** check box.

**Step 5** Check the check box for each aging rule that you want to enable and specify the number of days after which the aging action will take place. See **Help** for information on individual aging rules.

**Step 6** For each aging rule that you enabled in Step 5, indicate whether you want users to be alerted by email before the aging action takes place. Then specify the number of days prior to the message aging action that users will be alerted.

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

For information on configuring which message aging policy is assigned to individual users and to templates, see the "Message Aging in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Changing a Message Aging Policy

To change settings in the Default System Policy or in any message aging policies that you have added, do the following procedure.

**Caution** Do not change settings in the **Do Not Age Messages** policy.

### To Change a Message Aging Policy

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then expand **Message Aging**, then select **Aging Policies**.

In Cisco Unity Connection Administration, expand **Message Storage**, then select **Message Aging Policy**.

**Step 2** Select the name of the policy that you want to change.

**Step 3** Change settings as applicable. See **Help** for information on individual fields.

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

For information on changing which message aging policy is assigned to individual users and to templates, see the "Message Aging in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Deleting a Message Aging Policy

If you want to delete a message aging policy, do the following procedure.

We recommend that you do not delete either the Default System Policy or the Do Not Age Messages policy. If you do not want to age messages, disable the Default System Policy instead of deleting it.

### To Delete a Message Aging Policy

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then expand **Message Aging**, then select **Aging Policies**.

In Cisco Unity Connection Administration, expand **Message Storage**, then select **Message Aging Policy**.

**Step 2** Check the check box next to the name of the policy that you want to delete.

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

**Step 4** Select **OK** to confirm.

# Configuring a Smart Host for Message Aging Alerts

To enable Cisco Unity Connection to send message aging alert emails to users, you must configure the Unity Connection server to relay messages through an SMTP smart host.

### To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Smart Host**.

**Step 2** On the **Smart Host** page, in the **Smart Host** field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

**Step 3** Select **Save**.

**Step 4** On your SMTP server application, configure an SMTP smart host to accept messages from the Unity Connection server. For instructions, see the documentation for the SMTP server application that you are using.

# Configuring Message Aging Alert Text

If you want to customize the **Subject Line** or **Body Text** of the message aging alert emails that are sent to users, do the following procedure.

### To Customize the Message Aging Alert Text

**Step 1** In Cisco Unity Connection Administration, expand **Message Storage**, then expand **Message Aging**, then select **Aging Alert Text**.

**Step 2** On the **Edit Message Aging Alert Text** page, in the **Language** list, select the applicable language.

**Step 3** For each of the five message aging rules, determine whether you want to use the default text for the email **Subject Line** and **Body Text**. If you decide to customize a rule, continue with Step 4.

**Step 4** To customize text for a message aging rule, do the following sub-steps:

**a.** Uncheck the **Use Default Text** check box.

**b.** Enter text in the **Subject Line** and **Body Text** fields as applicable. See Table 26-3 for a list of available parameters.

**c.** Repeat a. through b. for each aging rule that you want to customize.

**Step 5** Select **Save**.

**Step 6** Repeat Step 2 through Step 5 for each language installed on the system.

*Table 26-3 Message Aging Alert Text Parameters*

| Parameter | Description |
|---|---|
| %ARRIVALTIME% | When the %ARRIVALTIME% parameter is used, it is replaced with the date and time the message was received. |
| %DAYSUNTIL% | When the %DAYSUNTIL% parameter is used, it is replaced with the number of days until the applicable message aging action will be applied to the message. |
| %MODIFICATIONTIME% | When the %MODIFICATIONTIME% parameter is used, it is replaced with the date and time that the message was last touched by the recipient or the system. (For example, the recipient touches the message by saving, deleting, or opening and then saving the messages as new. The system touches the message when a message aging rule moves a new message to the saved messages folder or moves a saved message to the deleted items folder.) |
| %RECIPIENT% | When the %RECIPIENT% parameter is used, it is replaced with the display name of the message recipient. |
| %RECIPIENT_EXTENSION% | When the %RECIPIENT_EXTENSION% parameter is used, it is replaced with the extension number of the mailbox of the message recipient.<br>This parameter might be useful if some users monitor multiple mailboxes. |
| %SENDER% | When the %SENDER% parameter is used, it is replaced with the display name of the sender of the message. |

## Configuring Message Aging When Single Inbox Is Configured

When single inbox is configured, messages that users delete by using Outlook are only moved to the Deleted Items folder in Outlook, not permanently deleted. When Unity Connection synchronizes with Exchange, messages that have been deleted in Outlook are moved to the Unity Connection Deleted Items folder. The messages are not permanently deleted from Unity Connection. We recommend that you configure message aging to permanently delete messages in the Deleted Items folder.

You can also configure message quotas, so that the Unity Connection conversation prompts users to delete messages when their mailboxes approach a specified size. See the "Specifying Mailbox Size Quotas in Cisco Unity Connection 10.x" section on page 26-1.

# Message Recording Expiration

The Message Recording Expiration feature guarantees that a voice message that is stored on the Cisco Unity Connection server cannot be listened to after it reaches a set expiration date, regardless of whether the message has been forwarded to another Unity Connection recipient. Message Recording Expiration is a systemwide setting, and thus cannot be applied only to a subset of users.

You set the number of days after which messages arrive that they will expire. At expiration, message recordings are automatically replaced with a decoy recording that says, "The message has expired."

Typically, message aging rules are sufficient for enforcing message-retention policies. Note, however, that when a message is forwarded, the forwarded message is considered a new message and its age is reset. If you are concerned that users may forward messages in an attempt to circumvent the message-retention policy, consider enabling the Message Recording Expiration feature. The message recording and transcription (if any) expire based on the date that the original copy of the message arrived, regardless of user forwarding.

By default, the Message Recording Expiration feature is not enabled. You can enable and configure the feature on the **Message Storage Settings > Message Aging > Message Recording Expiration** page in Cisco Unity Connection Administration.

If you enable the **Message Recording Expiration** feature, we recommend that you configure the expiration time frame to be two to three times longer than the message aging time frame. (For example, if all of your messages are marked secure by default and you have a message aging policy set to permanently delete all secure messages older than 60 days, configure message recordings to expire in 180 days.)

**Note** The **Message Recording Expiration** feature does not apply to messages that have been forwarded to personal email addresses or to message recordings that have been saved locally to user workstations.

To prevent users from saving local copies or forwarding voice messages to personal email addresses, consider configuring Unity Connection to mark all messages as secure.Unity Connection applies the **Message Recording Expiration** feature to messages in the mailboxes of recipients that are homed on the Unity Connection server. For example, if User A homed on Unity Connection server A sends a message to User B homed on Unity Connection server B, the message will be subject to message expiration only if the **Message Recording Expiration** feature is enabled on server B.

# Setting Up HTML, SMTP, and SMS (SMPP) Message Notifications in Cisco Unity Connection 10.x

Cisco Unity Connection can notify a user of new messages by calling a phone or pager. Additionally, you can set up Unity Connection to send message and calendar event notifications in the form of text messages to text pagers and text-compatible mobile phones by using SMTP.

Unity Connection configured with the SMTP smart host settings can also be used to send the HTML notifications from Cisco Unity Connection Administration.

You can also set up Unity Connection to send message and calendar event notifications in the form of SMS messages to wireless devices by using SMPP.

See the following sections:

- Setting Up HTML or SMTP Message Notifications in Cisco Unity Connection 10.x, page 27-1
- Setting Up SMS (SMPP) Message Notifications in Cisco Unity Connection 10.x, page 27-2

(For information on setting up message notifications to a phone or pager, see the "Phone and Pager Notification Devices" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html. )

## Setting Up HTML or SMTP Message Notifications in Cisco Unity Connection 10.x

By using SMTP, Cisco Unity Connection can send an HTML or text notification to notify users that they have received a new message. The HTML notification use SMTP to notify the users that they have received a new voice message via email. The HTML notifications are used only for voice messages. In case of the text notifications, the users are also notified for the calendar events. In addition, the text notifications can be sent to any device or email client that supports SMTP, for example, email addresses, mobile phones, and text pagers.

To enable Unity Connection to send notifications by using SMTP, the Unity Connection server must be configured to relay messages through a smart host. If Unity Connection is configured to deliver the HTML or text notifications but has not been configured to relay messages to a smart host, the notification attempt fails and the notification is put in the Unity Connection SMTP Server badmail folder.

When a Unity Connection user receives a new message, Unity Connection can send an HTML or text notification to an email address.

**Note** If your site includes a Unity Connection cluster, make sure that the SMTP Domain Address resolves to IP addresses of both the publisher and subscriber servers. The SMTP Domain Address facilitates to reach the cluster subscriber server when the publisher is down or vice versa. To configure the SMTP domain, go to the **System Settings > SMTP Configuration > Server** page.

To enable HTML or SMTP notifications, do the following tasks:

1. Configure the SMTP smart host to accept messages from the Unity Connection server. See the documentation for the SMTP server application that you are using.
2. Configure the Unity Connection server. See the "To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host" procedure on page 27-2.
3. Configure Unity Connection users or templates. See the "SMTP-Compatible Notification Devices" and "HTML-Compatible Notification Devices" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

   Alternatively, the users can set up their own HTML or SMTP-compatible devices by using the Unity Connection Messaging Assistant. See the "Managing Message Notification" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html.

### To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then select **Smart Host**.

**Step 2** On the **Smart Host** page, in the **Smart Host** field, enter the IP address or fully qualified domain name of the SMTP smarthost server, for example, https://ucbu-cisco-vmxyz.cisco.com. (Enter the fully qualified domain name of the server only if DNS is configured.)

**Step 3** Select **Save**.

# Setting Up SMS (SMPP) Message Notifications in Cisco Unity Connection 10.x

With the services and information provided by a wireless carrier, mobile messaging service provider or similar company, Cisco Unity Connection can use the Short Message Peer-to-Peer (SMPP) protocol to send message notifications in the Short Message Service (SMS) format to mobile phones and other SMS-compatible devices when users receive new messages. SMS is a "store and forward service," which means that messages are not sent directly to the device used by the message recipient. Instead, an application like Unity Connection—known as an External Short Message Entity (ESME)—submits a message to the SMS Center (SMSC). The SMSC then forwards the message to the device.

### Advantages Over SMTP Message Notifications

An advantage of using SMS is that the user device often receives message notifications much faster than when using SMTP. The user device does not have to be on the wireless network at the time that Unity Connection sends the message to the SMSC, nor when the SMSC forwards it. The wireless network holds the SMS messages until the device is available; when the device is available, the delivery of the queued messages to the device takes just a few seconds. In addition, you can configure Unity Connection so that each notification message replaces the previous one. Note that this functionality may not be supported by all mobile service providers.

### SMS Message Length Limitations

An SMS message is a short text message. The acceptable message length for an SMS message varies depending on the service provider, the character set used to compose the message text, and the specific characters used in the message text. The message count (assuming that users choose to include the message count) is not included in the total message length.

Character sets available include:

- Default Alphabet (GSM 3.38), 7-bit characters
- IA5/ASCII, 7-bit characters
- Latin 1 (ISO-8859-1), 8-bit characters
- Japanese (JIS), multi-byte characters
- Cyrillic (ISO-8859-5), 8-bit characters
- Latin/Hebrew (ISO-8859-8), 8-bit characters
- Unicode (USC-2), 16-bit characters
- Korean (KS C 5601), multi-byte characters

For 7-bit character sets, a maximum of 160 characters can fit into an SMS message; for 8-bit character sets, the limit is 140 characters; for 16-bit character sets, the limit is 70 characters; for multi-byte character sets, the limit is somewhere between 70 and 140 characters, depending on which characters make up the text of the message. (For multi-byte character sets, most characters are 16 bits; some of the more common characters are eight bits.)

**Note** Not all mobile phones support all character sets; most support the GSM 3.38 default alphabet.

### Cost Considerations

When setting up SMS (SMPP) message notifications, consider that service providers typically charge for each SMS message or group of messages sent. Thus, the more SMS (SMPP) message notifications that Unity Connection sends to user devices, the higher the costs to your organization. For this reason, you may want to restrict the use of this feature to a group of users (you can do so by assigning owners to the SMPP providers that you create), or you may want to ask users to limit the number of message notifications that they receive by message type or urgency. For example, users can specify in the Unity Connection Messaging Assistant that Unity Connection sends message notifications only when new urgent voice messages arrive.

# Task List for Setting Up SMS (SMPP) Message Notifications

To enable SMS (SMPP) message notifications for users with SMS-compatible devices, do the following tasks:

1. Set up an account with a mobile messaging service provider that offers SMS messaging. Unity Connection works with any service provider that supports the SMPP version 3.3 or SMPP version 3.4 protocols.
2. Gather the information needed to allow Unity Connection to communicate with the SMPP server at the SMSC affiliated with your contracted service provider, and enter the information on the SMPP Provider page. See the "To Set Up an SMPP Provider" procedure on page 27-4.
3. When the Unity Connection server is set up behind a firewall, configure the TCP port that is used by the SMPP server when connecting to Unity Connection to allow incoming and outgoing communication between Unity Connection and the SMPP server.
4. Enable SMS (SMPP) message notification and set up an SMS-compatible device to receive notifications for a user account, and then test to see if the device receives the SMS (SMPP) notification as expected. If notifications are not working, confirm that you entered the settings on the SMPP Provider page as indicated in the documentation that your service provider gave you. Contact your service provider for assistance, as needed.

   Procedures for setting up a device and enabling SMS (SMPP) notifications are in the "SMS-Compatible Notification Devices" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.
5. Repeat the previous task for additional users.

### To Set Up an SMPP Provider

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **SMPP Providers**.

**Step 2** On the **Search SMPP Providers** page, select **Add New**.

**Step 3** On the **New SMPP Provider** page, verify that the **Enable** check box is checked.

**Step 4** Enter a **Name** for the provider.

**Step 5** Enter the **System ID** given to you by your service provider.

**Step 6** Enter a **Host Name/Address**, which is the SMSC Host name or IP address given to you by your service provider.

**Step 7** If applicable, enter the **Source Address** given to you by the service provider. If your provider did not specify a value, leave the field blank.

**Step 8** Set the Owner, as follows:

- To restrict provider use, select a user as owner of the selected SMPP provider. Select **User** and then select the applicable user in the list.
- To allow the SMPP provider to be used by all users with associated SMS (SMPP) notification devices at a location, select **System** as owner of the selected SMPP provider.

**Step 9** Select **Save**.

**Step 10** On the **Edit SMPP Provider** page, enter the Port, which is the port number that is used by the SMSC to listen for incoming connections.

**Note** The port number used by SMSC to listen for incoming connections should be in range of >100 and <=99999.

**Step 11** Enter the **Password** given to you by your service provider.

**Step 12** If applicable, enter the **System Type, Address TONs**, and **Address NPIs** given to you by the service provider. If your provider did not specify values, leave the fields blank.

**Step 13** If applicable, in the **Data Coding** list, select the character set that you want each SMS message converted to when the messages are sent to the SMS device. (If your provider did not specify a value, select **Default Alphabet**.) For multilingual systems, consider creating a separate SMPP provider for each character set that you want to offer to users.

**Step 14** Enter additional settings, as applicable.

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

# Configuring SSL in Cisco Unity Connection 10.x

This chapter contains information on creating a certificate signing request, issuing an SSL certificate (or having it issued by an external certification authority), and installing the certificate on the Cisco Unity Connection server to secure Cisco Unity Connection Administration, Cisco Personal Communications Assistant (Cisco PCA) and IMAP email client access to Cisco Unity Connection.

The Cisco PCA website provides access to the web tools that users use to manage messages and personal preferences with Unity Connection.

**Note** IMAP client access to Unity Connection voice messages is a licensed feature.

See the following sections:

- Deciding Whether to Create and Install an SSL Certificate in Cisco Unity Connection 10.x, page 28-1
- Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 10.x, page 28-2
- Installing Microsoft Certificate Services (Windows Server 2003 Only) in Cisco Unity Connection 10.x, page 28-5

## Deciding Whether to Create and Install an SSL Certificate in Cisco Unity Connection 10.x

When you install Cisco Unity Connection, a local certificate is automatically created and installed to secure communication between the Cisco PCA and Unity Connection, and between IMAP email clients and Unity Connection. This means that all network traffic (including usernames, passwords, other text data, and voice messages) between the Cisco PCA and Unity Connection is automatically encrypted, and network traffic between IMAP email clients and Unity Connection is automatically encrypted if you enable encryption in the IMAP clients. However, if you want to reduce the risk of man-in-the-middle attacks, do the procedures in this chapter.

If you decide to install an SSL certificate, we recommend that you also consider adding the trust certificate of the certification authority to the Trusted Root Store on user workstations. Without the addition, the web browser displays security alerts for users who access the Cisco PCA and for users who access Unity Connection voice messages with some IMAP email clients.

(For information on managing security alerts, see the "Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection 10.x" section in the "Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection 10.x" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 10.x*. For information on configuring supported IMAP email clients, see the "Configuring an Email Account to Access Cisco Unity Connection 10.x Voice Messages" chapter of the same guide. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_setup/guide/10xcucuwsx.html .)

# Securing Cisco Unity Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 10.x

Do the following tasks to create and install an SSL server certificate to secure Cisco Unity Connection Administration, Cisco Personal Communications Assistant, and IMAP email client access to Cisco Unity Connection:

1. If you are using Microsoft Certificate Services to issue certificates, install Microsoft Certificate Services. For information on installing Microsoft Certificate Services on a server running Windows Server 2003, see the "Installing Microsoft Certificate Services (Windows Server 2003 Only) in Cisco Unity Connection 10.x" section on page 28-5. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, refer to Microsoft documentation.

   If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Task 2.

   If you are using an external certification authority to issue certificates, skip to Task 2.

**Note** If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 2.

2. If a Unity Connection cluster is configured, run the `set web-security` CLI command on both Unity Connection servers in the cluster and assign both servers the same alternate name. The alternate name will automatically be included in the certificate signing request and in the certificate. For information on the `set web-security` CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
3. If a Unity Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Task 2. List the publisher server first. This allows all IMAP email applications and the Cisco Personal Communications Assistant to access Unity Connection voice messages by using the same Unity Connection server name.
4. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external CA. Do the "To Create and Download a Certificate Signing Request" procedure on page 28-3.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

5. If you are using Microsoft Certificate Services to export the issuer certificate and to issue the server certificate, do the procedure in the "Exporting the Issuer Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only) in Cisco Unity Connection 10.x" section on page 28-6.

   If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

   If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Task 6.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

6. Upload the issuer certificate and the server certificate to the Unity Connection server. Do the "To Upload the Issuer and Server Certificates to the Cisco Unity Connection Server" procedure on page 28-4.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

7. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Unity Connection IMAP Server Service" procedure on page 28-5.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

8. To prevent users from seeing a security alert whenever they access Unity Connection by using Connection Administration, the Cisco PCA, or an IMAP email client, do the following tasks on all computers from which users will access Unity Connection:

   – Import the server certificate that you uploaded to the Unity Connection server in Task 6. into the certificate store. The procedure differs based on the browser or IMAP email client. For more information, see the documentation for the browser or IMAP email client.

   – Import the server certificate that you uploaded to the Unity Connection server in Task 6. into the Java store. The procedure differs based on the operating system running on the client computer. For more information, see the operating system documentation and the Java Runtime Environment documentation.

### To Create and Download a Certificate Signing Request

**Step 1** On the Cisco Unity Connection server, sign in to Cisco Unified Operating System Administration.

**Step 2** On the **Security** menu, select **Certificate Management**.

**Step 3** On the **Certificate List** page, select **Generate CSR**.

**Step 4** On the **Generate Certificate Signing Request** page, in the **Certificate Name** list, select **tomcat**.

**Step 5** Select **Generate CSR**.

**Step 6** When the **Status** area displays a message that the CSR was successfully generated, select **Close**.

**Step 7** On the **Certificate List** page, select **Download CSR**.

**Step 8** On the **Download Certificate Signing Request** page, in the **Certificate Name** list, select **tomcat**.

**Step 9** Select **Download CSR**.

**Step 10** In the **File Download** dialog box, select **Save**.

**Step 11** In the **Save As** dialog box, in the **Save As Type** list, select **All Files**.

**Step 12** Save the file **tomcat.csr** to a location on the server on which you installed Microsoft Certificate Services or on a server that you can use to send the CSR to an external certification authority.

**Step 13** On the **Download Certificate Signing Request** page, select **Close**.

### To Upload the Issuer and Server Certificates to the Cisco Unity Connection Server

**Step 1** On the Cisco Unity Connection server on which you created the certificate signing request, sign in to Cisco Unified Operating System Administration.

**Step 2** On the **Security** menu, select **Certificate Management**.

**Note** If you select **Find** and display a list of the certificates currently installed on the server, you will see an existing, automatically generated, self-signed certificate for Tomcat. That certificate is unrelated to the Tomcat certificates that you upload in this procedure.

**Step 3** Upload the issuer certificate:

a. On the **Certificate List** page, select **Upload Certificate**.

b. On the **Upload Certificate** page, in the **Certificate Name** list, select **tomcat-trust**.

c. Leave the **Root Certificate** field blank.

d. Select **Browse**, and browse to the location of the issuer CA certificate.

   If you used Microsoft Certificate Services to issue the certificate, this is the location of the issuer certificate that you exported in the "To Export the Issuer Certificate and to Issue the Server Certificate" procedure on page 28-6.

   If you used an external certification authority to issue the certificate, this is the location of the issuer CA certificate that you received from the external certification authority.

e. Select the name of the file.

f. Select **Open**.

g. On the **Upload Certificate** page, select **Upload File**.

h. When the **Status** area reports that the upload succeeded, select **Close**.

**Step 4** Upload the server certificate:

a. On the **Certificate List** page, select **Upload Certificate**.

b. On the **Upload Certificate** page, in the **Certificate Name** list, select **tomcat**.

c. In the **Root Certificate** field, enter the filename of the issuer certificate that you uploaded in Step 3.

d. Select **Browse**, and browse to the location of the server certificate.

   If you used Microsoft Certificate Services to issue the certificate, this is the location of the server certificate that you issued in the "To Export the Issuer Certificate and to Issue the Server Certificate" procedure on page 28-6.

   If you used an external certification authority to issue the certificate, this is the location of the server certificate that you received from the external certification authority.

e. Select the name of the file.

f. Select **Open**.

g. On the **Upload Certificate** page, select **Upload File**.

h. When the **Status** area reports that the upload succeeded, select **Close**.

**Step 5** Restart the **Tomcat** service (the service cannot be restarted from Cisco Unified Serviceability):

a. Sign in to the Unity Connection server by using an SSH application.

b. Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

#### To Restart the Unity Connection IMAP Server Service

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

**Step 2** On the **Tools** menu, select **Service Management**.

**Step 3** In the **Optional Services** section, for the **Unity Connection IMAP Server** service, select **Stop**.

**Step 4** When the **Status** area displays a message that the **Unity Connection IMAP Server** service was successfully stopped, select **Start** for the service.

# Installing Microsoft Certificate Services (Windows Server 2003 Only) in Cisco Unity Connection 10.x

If you want to use a third-party certificate authority to issue SSL certificates, or if Microsoft Certificate Services is already installed, skip this section.

Do the procedure in this section if you want to use Microsoft Certificate Services to issue your own certificate and if you want to install the application on a server running Windows Server 2003.

If you want to install a root certification authority (the generic term for Microsoft Certificate Services) on a Windows Server 2008 server, refer to the Windows Server 2008 online help.

#### To Install the Microsoft Certificate Services Component

**Step 1** On any server whose DNS name (FQDN) or IP address can be resolved by all client computers that will use the Cisco PCA or that will use an IMAP client to access Cisco Unity Connection voice messages, sign in to Windows by using an account that is a member of the local administrators group.

**Step 2** On the **Windows Start** menu, select **Settings > Control Panel > Add or Remove Programs**.

**Step 3** In the left pane of the **Add or Remove Programs** control panel, select **Add/Remove Windows Components**.

**Step 4** In the **Windows Components** dialog box, check the **Certificate Services** check box. Do not change any other items.

**Step 5** When the warning appears about not being able to rename the computer or to change domain membership, select **Yes**.

**Step 6** Select **Next**.

**Step 7** On the **CA Type** page, select **Stand-alone Root CA**, and select **Next**. (A stand-alone certification authority (CA) is a CA that does not require Active Directory.)

**Step 8** On the **CA Identifying Information** page, in the **Common Name for This CA** field, enter a name for the certification authority.

**Step 9** Accept the default value in the **Distinguished Name Suffix** field.

**Step 10** For **Validity Period**, accept the default value of **5 Years**.

**Step 11** Select **Next**.

**Step 12** On the **Certificate Database Settings** page, select **Next** to accept the default values.

If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, select **Yes** to stop the services.

**Step 13** If you are prompted to insert the Windows Server 2003 disc into the drive, do so.

**Step 14** In the **Completing the Windows Components Wizard** dialog box, select **Finish**.

**Step 15** Close the **Add or Remove Programs** dialog box.

# Exporting the Issuer Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only) in Cisco Unity Connection 10.x

Do the following procedure only when you are using Microsoft Certificate Services to issue the certificate.

### To Export the Issuer Certificate and to Issue the Server Certificate

**Step 1** On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the **Domain Admins** group.

**Step 2** On the Windows Start menu, select **Programs > Administrative Tools > Certification Authority**.

**Step 3** In the left pane, expand **Certification Authority (Local) > <Certification authority name>**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the "To Install the Microsoft Certificate Services Component" procedure on page 28-5.

**Step 4** Export the issuer certificate:

a. Right-click the name of the certification authority, and select **Properties**.

b. On the **General** tab, select **View Certificate**.

c. Select the **Details** tab.

d. Select **Copy to File**.

e. On the **Welcome to the Certificate Export Wizard** page, select **Next**.

f. On the **Export File Format** page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.

g. On the File to Export page, enter a path and filename for the .cer file. Select a network location that you can access from the Unity Connection server.

   Write down the path and filename. You will need it in a later procedure.

h. Follow the onscreen prompts until the wizard has finished the export.

i. Select **OK** to close the **Certificate** dialog box, and select **OK** again to close the Properties dialog box.

**Step 5** Issue the server certificate:

a. Right-click the name of the certification authority, and select **All Tasks > Submit New Request**.

b. Browse to the location of the certificate signing request file that you created in the "To Create and Download a Certificate Signing Request" procedure on page 28-3, and double-click the file.

c. In the left pane of **Certification Authority,** select **Pending Requests**.

d. Right-click the pending request that you submitted in b., and select **All Tasks > Issue**.

e. In the left pane of **Certification Authority,** select **Issued Certificates**.

f. Right-click the new certificate, and select **All Tasks > Export Binary Data**.

g. In the **Export Binary Data** dialog box, in the Columns that Contain Binary Data list, select **Binary Certificate**.

h. Select **Save Binary Data to a File**.

i. Select **OK**.

j. In the **Save Binary Data** dialog box, enter a path and filename. Select a network location that you can access from the Cisco Unity Connection server.

   Write down the path and filename. You will need it in a later procedure.

k. Select **OK**.

**Step 6** Close **Certification Authority**.

# Setting Up Broadcast Messaging in Cisco Unity Connection 10.x

System broadcast messages are recorded announcements that are sent to everyone in an organization. You determine whether users can send and/or update broadcast messages, and set up a way for them to do so by using the Cisco Unity Connection Broadcast Message Administrator. (By default, Cisco Unity Connection users are not enabled to send broadcast messages.)

See the following sections:


- How System Broadcast Messages Work in Cisco Unity Connection 10.x, page 29-1
- Task List for Offering Broadcast Messaging to Users in Cisco Unity Connection 10.x, page 29-2
- Enabling Phone Access to the Broadcast Message Administrator in Cisco Unity Connection 10.x, page 29-2
- Using the Broadcast Message Administrator in Cisco Unity Connection 10.x, page 29-6
- Changing Broadcast Message Administrator Defaults in Cisco Unity Connection 10.x, page 29-7


## How System Broadcast Messages Work in Cisco Unity Connection 10.x

Although system broadcast messages sound similar to regular voice messages, they are not simply voice messages that are sent to a large distribution list. They are unique in the following ways:

- System broadcast messages are played immediately after users sign in to Cisco Unity Connection by phone—even before they hear message counts for new and saved messages. After signing in, users hear how many system broadcast messages they have and Unity Connection begins playing them.
- For each system broadcast message, the sender specifies how long Unity Connection broadcasts the message. The sender can specify that a system broadcast message is “active” for a day, a week, a month—even indefinitely. A user hears the system broadcast message the first time that he or she signs in to Unity Connection during the period that the message is active.
- Users must listen to a system broadcast message in its entirety before Unity Connection allows them to hear new and saved messages or to change setup options. Users cannot fast-forward or skip a system broadcast message.

- If a user hangs up before playing the entire system broadcast message, the message plays again the next time that the user signs in to Unity Connection by phone (assuming that the message is still active).
- When a user has finished playing a system broadcast message, the message can either be replayed or permanently deleted. Users cannot respond to, forward, or save system broadcast messages.
- Users can receive an unlimited number of system broadcast messages.
- Users receive system broadcast messages even when they exceed their mailbox size limits and are no longer able to receive other messages. Because of the way that the messages are stored on the Unity Connection server, they are not included in the total mailbox size for each user.
- New users hear all active system broadcast messages immediately after they enroll as Unity Connection users.
- By design, system broadcast messages do not trigger message waiting indicators (MWIs) on user phones. They also do not trigger message notifications for alternative devices, such as a pager or another phone.
- Users hear broadcast messages only when listening to messages by phone. Users do not receive system broadcast messages when listening to messages in the Cisco Unity Connection Web Inbox, Messaging Inbox, an RSS reader, IMAP clients, Cisco Unified Personal Communicator, or Cisco Unified Messaging with IBM Lotus Sametime.
- When single inbox is configured, broadcast messages are excluded from synchronization between Unity Connection and Exchange.
- Unity Connection does not respond to voice commands while playing broadcast messages. When using the voice-recognition input style, users will need to use key presses to either replay or delete the broadcast message.

# Task List for Offering Broadcast Messaging to Users in Cisco Unity Connection 10.x

To allow users to send and/or update broadcast messages, do the following tasks in the order presented:

1. Set up a way for users to access the Broadcast Message Administrator. See the "Enabling Phone Access to the Broadcast Message Administrator in Cisco Unity Connection 10.x" section on page 29-2.
2. Enable user accounts or a template to send and update system broadcast messages. See the "Broadcast Messages" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Enabling Phone Access to the Broadcast Message Administrator in Cisco Unity Connection 10.x

To send a system broadcast message, Cisco Unity Connection users sign in to the Broadcast Message Administrator, which is a special conversation that allows them to send and update system broadcast messages.

You can give users access to the Broadcast Message Administrator in one of the following ways:

- Configure a Custom Keypad Mapping conversation—Use the Custom Keypad Mapping tool to map a key to the Broadcast Message Administrator Conversation so that it is offered to users from the main menu. See the "Custom Keypad Mapping Tool in Cisco Unity Connection 10.x" chapter for details.
- Create a call handler—See the "Creating a Call Handler to Send Users to the Broadcast Message Administrator" section on page 29-3.
- Set up a one-key dialing option—See the "Setting Up a One-Key Dialing Option to Send Users to the Broadcast Message Administrator" section on page 29-4.
- Set up a phone number and routing rule—See the "Setting Up a Special Phone Number and Routing Rule to Send Users to the Broadcast Message Administrator" section on page 29-5.

# Creating a Call Handler to Send Users to the Broadcast Message Administrator

You can create a new call handler, assign a unique extension to it, and specify the Broadcast Message Administrator as the destination to which Cisco Unity Connection sends the user after hearing the greeting. To make the transfer quick and seamless to users, select a blank greeting for the call handler.

### To Create a Call Handler to Send Users to the Broadcast Message Administrator

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, select **Add New**.

**Step 3** On the **New Call Handler** page, enter a display name and the extension that users can dial to reach the call handler.

**Step 4** Select the call handler template on which to base the new call handler.

**Step 5** Select **Save**.

**Step 6** On the **Edit Call Handler Basics** page, on the **Edit** menu, select **Greetings**.

**Step 7** On the **Greetings** page, select the **Standard** greeting.

**Step 8** On the **Edit Greeting** page, in the **Callers Hear** section, select **Nothing**. (Alternatively, you can select **My Personal Recording** and record a greeting that introduces the caller to the **Broadcast Message Administrator** conversation.)

**Step 9** In the **After Greeting** section, select **Conversation** and then select **Broadcast Message Administrator**.

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

**Step 11** If you want to set up a one-key dialing option for the call handler, so that callers can reach the Broadcast Message Administrator by pressing a key while listening to the greeting, continue with the "To Set Up a One-Key Dialing Option from a Call Handler for Accessing the Broadcast Message Administrator" procedure on page 29-4.

# Setting Up a One-Key Dialing Option to Send Users to the Broadcast Message Administrator

You can specify that Cisco Unity Connection sends a caller to the **Broadcast Message Administrator** (on the **Caller Input** page for any call handler or user greeting) when a caller presses a particular key during the greeting.

To set up a one-key dialing option for accessing the Broadcast Message Administrator, use one of the following procedures:

- To Set Up a One-Key Dialing Option from a Call Handler for Accessing the Broadcast Message Administrator, page 29-4
- To Set Up a One-Key Dialing Option from a User Greeting for Accessing the Broadcast Message Administrator, page 29-5

### To Set Up a One-Key Dialing Option from a Call Handler for Accessing the Broadcast Message Administrator

**Step 1** In Cisco Unity Connection Administration, expand **Call Management**, then select **System Call Handlers**.

**Step 2** On the **Search Call Handlers** page, in the **Search Results** table, select the display name of the applicable call handler.

If you want to set up access to the **Broadcast Message Administrator** from the opening greeting, select the **Opening Greeting** call handler. Or select the display name of another call handler that you have created for this purpose.

**Note** If the call handler that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Call Handler Basics** page, on the **Edit** menu, select **Caller Input**.

**Step 4** On the **Caller Input** page, in the **Caller Input Keys** table, select the applicable phone keypad key.

**Step 5** On the **Edit Caller Input** page for the key that you have selected, check the **Ignore Additional Input (Locked)** check box.

**Note** If you are setting up one-key dialing from the **Opening Greeting**, ensure that the phone keypad key that you select to lock is not the first digit of any of the extensions in your system. If it is, locking the key prevents callers from dialing an extension while listening to the Opening Greeting. Instead, select a key that is not the first digit of any extension.

**Step 6** Select **Conversation**, and then select **Broadcast Message Administrator**.

**Step 7** Optionally, you can rerecord the greeting to mention the key that callers can press in the call handler greeting. (For example, "...for the Cisco Unity Connection Broadcast Message Administrator, press 3.")

**Step 8** Select **Save**.

### To Set Up a One-Key Dialing Option from a User Greeting for Accessing the Broadcast Message Administrator

**Step 1** In Cisco Unity Connection Administration, select **Users**.

**Step 2** On the **Search Users** page, in the **Search Results** table, select the alias of the applicable user.

**Note** If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **Caller Input**.

**Step 4** On the **Caller Input** page, in the **Caller Input Keys** table, select the applicable phone keypad key.

**Step 5** On the **Edit Caller Input** page for the key that you have selected, check the **Ignore Additional Input (Locked)** check box.

**Step 6** Select **Conversation**, and then select **Broadcast Message Administrator**.

**Step 7** Optionally, you can rerecord the greeting to mention the key that callers can press while listening to the user greeting. (For example, "...for the Cisco Unity Connection Broadcast Message Administrator, press 3.")

**Step 8** Select **Save**.

## Setting Up a Special Phone Number and Routing Rule to Send Users to the Broadcast Message Administrator

See the documentation for the phone system to set up a new phone number. Then use the following procedure to create a routing rule that sends any call that arrives for the new number to the Broadcast Message Administrator conversation.

### To Add a Routing Rule to Send Callers to the Broadcast Message Administrator

**Step 1** In Cisco Unity Connection Administration, expand **Call Management > Call Routing**, then select **Direct Routing Rules**.

**Step 2** On the **Direct Routing Rules** page, select **Add New**.

**Step 3** On the **New Direct Routing Rule** page, enter a display name for the new routing rule, and select **Save**.

**Step 4** On the **Edit Direct Routing Rule** page, confirm that the **Status** is set to **Active**.

**Step 5** In the **Send Call To** field, select **Conversation**, and then select **Broadcast Message Administrator**.

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

**Step 7** In the **Routing Rule Conditions** table, select **Add New**.

**Step 8** On the **New Direct Routing Rule Condition** page, select **Dialed Number**, select **Equals**, and then enter the phone number that has been set up for access to the Broadcast Message Administrator.

**Step 9** Select **Save**.

**Step 10** On the **Direct Routing Rule** menu, select **Direct Routing Rules**.

**Step 11** On the **Direct Routing Rules** page, verify that the new routing rule is in an appropriate position with the other routing rules in the table. If you want to change the rule order, continue with Step 12.

**Step 12** Select **Change Order**.

**Step 13** On the **Edit Direct Routing Rule Order** page, select the name of the rule you want to reorder, and select the **Up** or **Down** arrow until the rules appear in the correct order. Select **Save**.

**Step 14** Distribute the new number to callers who are enabled to send and/or update system broadcast messages.

# Using the Broadcast Message Administrator in Cisco Unity Connection 10.x

Users whose account settings allow them to send and update system broadcast messages can use the Broadcast Message Administrator to do the following tasks:

- Record and send one or more system broadcast messages.
- Define when a system broadcast message becomes active and for how long. Unless otherwise specified by the sender, each message is set by default to broadcast immediately and to remain active for 30 days. Senders can set a future date and time for the message to be broadcast, and can specify that a system broadcast message is "active" for a day, a week, a month—even indefinitely.

**Note** Date and times reflect the time zone for the user who sends the message, not those who receive it.

To change default behavior for the Broadcast Message Administrator, see the "Changing Broadcast Message Administrator Defaults in Cisco Unity Connection 10.x" section on page 29-7.

**Note** If a sender hangs up or is disconnected while creating a broadcast message, but before sending it, Cisco Unity Connection deletes the recording.

Users who are able to update system broadcast messages can use the Broadcast Message Administrator to do the following tasks on the local Unity Connection server:

- Review active messages. (If there is more than one active message, the Broadcast Message Administrator presents them in order based on the start date and time, starting with the newest messages.)
- Change the end date and time for active messages.
- Change or add to a recording for future messages. (Note that Unity Connection enforces the total message length limit even when material is added to a message.)
- Change the start date and time or the end date and time for future messages. (Note that the end date and time does not adjust automatically if senders change the start date and time but do not change the end date and time.)
- Delete active and future messages. (Note that Unity Connection does not report which users have already played an active message.)

# Changing Broadcast Message Administrator Defaults in Cisco Unity Connection 10.x

Default behavior for the Broadcast Message Administrator is controlled by settings on the **System Settings > Advanced > Conversations** page in Cisco Unity Connection Administration. Optionally, you can make changes to the system defaults, as follows:

- **Retention Period**—Indicates how long Unity Connection retains expired system broadcast messages on the server. By default, Unity Connection purges the WAV file and any data associated with a message 30 days after its end date and time. To change the retention period for expired broadcast messages, enter a number from 1 to 60 days.
- **Default Active Days**—Indicates the number of days that a system broadcast message remains active when the sender does not specify an end date and time. The default is 30 days. To change how long a message without an end date and time remains active, enter a number from zero (0) to 365 days. A value of zero (0) days means that messages that are sent without a specified end date and time remain active indefinitely.
- **Maximum Recording Length**—Indicates the maximum length allowed for system broadcast messages. By default, senders can record messages up to 300,000 milliseconds (5 minutes) in length. To change the maximum recording length, enter a number from 60,000 (1 minute) to 36,000,000 (60 minutes) milliseconds.
- **Play Oldest Message First**—Indicates the order in which Unity Connection presents system broadcast messages to users. By default, the check box is checked, which sets Unity Connection to play the oldest message first. To have the newest message played first, uncheck the check box.

# Managing System Distribution Lists in Cisco Unity Connection 10.x

**Note** System distribution lists are used to send voice messages to multiple users. The users that are members of a system distribution list typically are users who need the same information on a regular basis, such as employees in a department or members of a team.

The class of service of a user dictates whether the user can send messages to system distribution lists in Cisco Unity Connection.

See the following sections:


- Predefined System Distribution Lists in Cisco Unity Connection 10.x, page 30-1
- Creating System Distribution Lists in Cisco Unity Connection 10.x, page 30-2
- Modifying System Distribution Lists in Cisco Unity Connection 10.x, page 30-3
- Managing System Distribution List Members in Cisco Unity Connection 10.x, page 30-4
- Adding Alternate Names for a System Distribution List in Cisco Unity Connection 10.x, page 30-5
- Using Advanced Settings to Enable System Distribution List Access Lists in Cisco Unity Connection 10.x, page 30-6


# Predefined System Distribution Lists in Cisco Unity Connection 10.x

Cisco Unity Connection includes the following predefined system distribution lists, which you can modify but not delete:

| | |
|---|---|
| **All Voicemail Users** | When users with mailboxes are created, they are automatically added to the All Voicemail Users list.<br>When user accounts are deleted, they are automatically removed from this distribution list.<br>**Note** Default user accounts are not members of this list. |

| | |
|---|---|
| **Undeliverable Messages** | Users who are assigned to the Undeliverable Messages list receive messages left by outside callers for recipients whose mailboxes are not found or have been deleted, or non-delivery receipts (NDRs) that cannot be delivered to the original sender of a message.<br><br>By default, the UndeliverableMessagesMailbox user account is the only member of the Undeliverable Messages distribution list. We recommend that you add a user to the list, to monitor and reroute (as appropriate) any messages that are delivered to the list. |
| **All Voicemail-Enabled Contacts** | By default, the All Voicemail-Enabled Contacts list has no members. You may choose to add all VPIM contacts on the system as members of this list in order to address messages to the entire group. Also add any contact templates that are used to create (or automatically create) VPIM contacts, so that new VPIM contacts are automatically added as list members. |

# Creating System Distribution Lists in Cisco Unity Connection 10.x

Do the following procedure to create a single system distribution list in Cisco Unity Connection Administration.

**Tip** The Unity Connection Distribution List Builder tool can be used to bulk add users to a new or existing system distribution list based on a number of search criteria or by importing from a comma-separated value (CSV) file. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/Applications/CxN/PublicDistributionListBuilder/PublicDistributionListBuilder.html.

### To Create a System Distribution List

**Step 1** In Cisco Unity Connection Administration, expand **Distribution Lists**, then select **System Distribution Lists**.

**Step 2** On the **Search Distribution Lists** page, select **Add New**.

**Step 3** On the **New Distribution List** page, enter an alias and display name for the list.

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

**Step 5** On the **Edit Distribution List Basics** page, use the Media Master to record a name for the list. Users hear this recording as confirmation when they address messages to the list.

**Step 6** Optionally, enter an extension for the list.

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

**Step 8** On the **Edit** Menu, select **Distribution List Members**.

**Step 9** On the **Distribution List Members** page, select **Add User**.

**Step 10** In the **Available Users Search Results** table, check the check boxes next to the display names of the users to add to the list, then select **Add Selected**.

**Note** If the display names of the users that you want to add to the list do not appear in the search results table, you can increase the number of rows displayed on the page by changing the value specified in the **Rows Per Page** field. You can also set applicable parameters in the search fields at the top of the page, then select **Find** to display additional names in the table.

**Step 11** When you have added all members to the list, select **Close**.

**Note** You may need to select **Refresh** on the menu bar to see an updated list of distribution list members in the table.

# Modifying System Distribution Lists in Cisco Unity Connection 10.x

Do the applicable procedure:

- To Modify a System Distribution List, page 30-3
- To Modify System Distribution Lists in Bulk Edit Mode, page 30-4

You can also use the Bulk Administration Tool to modify system distribution lists. See the "Using the Cisco Unity Connection 10.x Bulk Administration Tool" appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x* for instructions (the guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html) .

### To Modify a System Distribution List

**Step 1** In Cisco Unity Connection Administration, expand **Distribution Lists**, then select **System Distribution Lists**.

**Step 2** On the **Search Distribution Lists** page, select the alias of the list you want to modify.

**Note** If the distribution list that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Distribution List Basics** page, change settings as applicable.

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

**Step 5** If you want to add or delete members from the distribution list, continue with the "To Add or Remove Users from a System Distribution List" procedure.

### To Modify System Distribution Lists in Bulk Edit Mode

**Step 1** On the **Search Distribution Lists** page, check the applicable distribution list check boxes, and select **Bulk Edit**.

If the distribution lists that you want to edit in bulk do not all appear on one **Search** page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable distribution lists. Then select **Bulk Edit**.

**Step 2** To make a change to a setting, check the check box to the left of the field name to select it, and then set the field as usual. Select **Help > This Page** to see descriptions of each setting.

**Note** The **Status** message at the top of the **Edit Distribution List Basics** page tells you how many distribution lists are being edited. Also note that the page is populated only with the fields that you are allowed to edit in bulk mode.

**Step 3** If applicable, set the **Bulk Edit Task Scheduling Fields** to schedule the **Bulk Edit** operation for a later date and/or time.

**Step 4** Select **Submit**.

**Step 5** If you want to add or delete members from a distribution list, continue with the "To Add or Remove Users from a System Distribution List" procedure.

# Managing System Distribution List Members in Cisco Unity Connection 10.x

You can add individual users directly to system distribution lists. When you delete a user account, Unity Connection automatically removes the user from any system distribution list of which the user is a member.

**Tip** The Unity Connection Distribution List Builder tool can be used to bulk add users to a new or existing system distribution list based on a number of search criteria or by importing from a comma-separated value (CSV) file. Download the latest version, and view training videos and Help at http://www.ciscounitytools.com/Applications/CxN/PublicDistributionListBuilder/PublicDistributionListBuilder.html.

You can also use the Bulk Administration Tool to modify system distribution list members. See the "Using the Cisco Unity Connection 10.x Bulk Administration Tool" appendix of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x* for instructions (the guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html) .

### To Add or Remove Users from a System Distribution List

**Step 1** In Cisco Unity Connection Administration, expand **Distribution Lists**, then select **System Distribution Lists**.

**Step 2** On the **Search Distribution Lists** page, select the alias of the list whose members you want to change.

**Note** If the distribution list does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Distribution List Basics** page, on the **Edit** menu, select **Distribution List Members**.

**Step 4** To add members to the list, continue with Step 5.

To remove members from the list, skip to Step 9.

**Step 5** To add members to the list, on the **Distribution List Members** page, select **Add User**.

**Note** You can also add other distribution lists as members of a distribution list. To add a distribution list, select **Add Distribution List**.

**Step 6** In the **Available Users Search Results** table, check the check boxes next to the display names of the users that you want to add to the list, then select **Add Selected**.

**Step 7** Select **Close**.

**Step 8** To see the updated list of members, on the menu bar, select **Refresh**.

**Step 9** To remove members from the list, on the **Distribution List Members** page, check the check boxes next to the display names of the users that you want to remove from the list, then select **Remove Selected**.

# Adding Alternate Names for a System Distribution List in Cisco Unity Connection 10.x

If the Cisco Unity Connection system uses the voice-recognition option, you can also specify alternate names for the display name that you give a system distribution list. Users say the display name when they use voice commands to address a message to the system distribution list by phone. Consider specifying alternate names if the display name is not pronounced the way it would be read, as may be the case with acronyms and abbreviations, or if some users are likely to try a different name to access a list. (For example, your list name for the Technical Support department is IT. You would add the pronunciation spelling “Eye Tea” as an alternate name. You could also add “Help Desk” as an alternate name.)

### To Add or Modify Alternate Names for System Distribution Lists

**Step 1** In Cisco Unity Connection Administration, expand **Distribution Lists**, then select **System Distribution Lists**.

**Step 2** On the **Search Distribution Lists** page, select the alias of the list for which you want to add alternate names.

**Note** If the distribution list does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Distribution List Basics** page, on the **Edit** menu, select **Alternate Names**.

**Step 4** On the **Edit Alternate Names** page, do any of the following:

- To add a new alternate name, in the **Add New Alternate Name** area, enter an alternate name in the **Display Name** field, then select **Add New**. When you have finished adding new alternate names, select **Save**.
- To modify an existing alternate name, in the **Edit Alternate Names** table, change the display name, then select **Save**.
- To delete an alternate name, check the check box next to the name, select **Delete Selected**, then select **OK** to verify that you want to delete the name.

# Using Advanced Settings to Enable System Distribution List Access Lists in Cisco Unity Connection 10.x

You can use search spaces and partitions to control who can send messages to system distribution lists—for example, you create a new partition called "Distribution Lists Partition," configure the lists that you want to control to use this partition, and assign a search space that includes this partition to users who have permission to send to the lists. However, if you have a large number of lists that each have a specific subset of users who are authorized to send messages to them, the search space approach may not scale well, and you may reach the limit on the number of partitions and search spaces that you can create on the server. As an alternative approach, you can configure advanced settings that allow you to set up individual access lists for each system distribution list that you want to control.

**Note** Only users and no other distribution lists in Unity Connection can be added as a member of system distribution list access list.

When you enable the access list feature, for each system distribution list that receives messages, you create a second system distribution list with an alias that is created from the alias of the original list plus a suffix that identifies the list as an access list. For example, to set up an access list for a system distribution list that has the alias allvoicemailusers, if the suffix is -accesslist, you create a second system distribution list with the alias allvoicemailusers-accesslist, and add as members of the access list any users who need to be able to send messages to allvoicemailusers. Note that users who are members of the access list must also have their search scope set to a search space that includes the partition of the system distribution list in order to address messages to the list.

Use the following task list to set up system distribution list access lists:

1. Configure the advanced settings that enable and control the access lists. Do the "To Enable and Configure System Distribution List Access Lists" procedure on page 30-7. If you are using Digital Networking to connect multiple Unity Connection servers, do this task on all of the servers.

**Caution** In a digital network, the values for the advanced settings that enable and control access lists must be configured identically on each location in the network in order for access lists to function properly.

2. For each system distribution list that you want to control with an access list, create a new system distribution list with an alias that is created from the alias of the original list plus a suffix that is defined in the System Distribution List Alias Suffix for Access Lists field. See the "Creating System Distribution Lists in Cisco Unity Connection 10.x" section on page 30-2.

### To Enable and Configure System Distribution List Access Lists

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, expand **Advanced**, then select **Messaging**.

**Step 2** To enable system distribution list access lists, check the **Use Access Lists to Control Who Can Send to System Distribution Lists** check box. (This check box is unchecked by default.)

**Step 3** To have Cisco Unity Connection continue to allow messages to be sent to system distribution lists that do not have access lists created for them, check the **Allow Delivery of Messages to System Distribution Lists That Have No Access Lis**t check box. Uncheck this check box to have Unity Connection reject all messages sent to system distribution lists that do not have an access list, and send a non-delivery receipt (NDR) to the message sender.

**Step 4** To specify the suffix that is used to distinguish access lists, enter a suffix in the **System Distribution List Alias Suffix for Access Lists** field. The default suffix is -accesslist.

**Step 5** Select **Save**.

# Managing Partitions and Search Spaces in Cisco Unity Connection 10.x

Partitions and search spaces provide a way to segregate the global dial and message addressing space within Cisco Unity Connection. A partition comprises a logical grouping of objects that are identifiable by extension, name or SMTP address (such as users, call handlers, and contacts). A search space contains an ordered list of partitions.

See the following sections:


- Overview of Partitions in Cisco Unity Connection 10.x, page 31-1
- Overview of Search Spaces in Cisco Unity Connection 10.x, page 31-2
- Default Partition and Search Space in Cisco Unity Connection 10.x, page 31-3
- Search Space Examples in Cisco Unity Connection 10.x, page 31-3
- How Search Spaces Work in Cisco Unity Connection 10.x, page 31-5
- Managing Partitions in Cisco Unity Connection 10.x, page 31-9
- Managing Search Spaces in Cisco Unity Connection 10.x, page 31-10
- Changing the System Default Partition and Search Space in Cisco Unity Connection 10.x, page 31-11
- Finding Objects that Belong to a Partition or Search Space in Cisco Unity Connection 10.x, page 31-11


## Overview of Partitions in Cisco Unity Connection 10.x

In Cisco Unity Connection, you create partitions as a way to group together objects to which callers and users can address messages or place calls while interacting with Unity Connection. One or more partitions can be grouped together as members of a search space, and a partition can be a member of more than one search space. The following types of objects belong to a partition:

- Users with mailboxes (primary extension)
- User alternate extensions
- Contacts (including VPIM contacts)
- System distribution lists
- System call handlers
- Directory handlers

- Interview handlers
- VPIM locations

In addition, you can use user templates, contact templates, and system call handler templates to set the partition membership for new objects of these types.

Extensions must be unique within a partition, although partitions can contain objects that do not have an associated extension (for example, some contacts and system distribution lists). The names of objects do not have to be unique within a partition. Administrator-defined contact phone numbers also do not need to be unique within a partition.

In general, objects can only be a member of a single partition, although a user can have a primary extension in one partition and an alternate extension in a different partition.

If there are alternate names defined for the user, the alternate names are available in each partition where the user has an extension.

**Note** When you change partition of an alternate extension in a bulk edit mode, the primary extension of the user is taken as an alternate extension. If primary extension already exist in the changed partition then it throws an error message with the duplicate extension.

# Overview of Search Spaces in Cisco Unity Connection 10.x

Search spaces are used to define the search scope of objects (users, distribution lists, and so on) that a user or outside caller can reach while interacting with Cisco Unity Connection. For example, the search scope that is applied to a user identifies which users, distribution lists, or VPIM contacts the user can address messages to. The search scope that is applied to a user also identifies which users and contacts the user can call by name dialing when using the voice-recognition conversation.

The following types of objects can use a search space for their search scope:

- Users with mailboxes
- Routing rules (both direct and forwarded)
- System call handlers
- Phone directory handlers
- Voice-enabled directory handlers
- VPIM locations

In addition, you can use user templates, contact templates, and system call handler templates to set the search scope for new objects of these types.

A search space is comprised of one or more ordered partitions. When Unity Connection searches for an object on behalf of a caller, it searches the partitions in the order in which they are arranged in the search space. While extensions must be unique within a partition, they do not need to be unique within a search space, so you can use search spaces to handle dial plans that have overlapping extensions.

For example, if there are two partitions, Regional_Office and Headquarters, each containing a Help Desk user with extension 4000, and a user at the regional office belongs to a search space that is assigned the two partitions in that order, when the user addresses to extension 4000, Unity Connection returns the Help Desk user from the Regional_Office partition. If another user at headquarters belongs to a second search space that is assigned the partitions in reverse order (Headquarters, then Regional_Office), this user hears the information for the Help Desk user in the Headquarters partition when addressing to extension 4000.

# Default Partition and Search Space in Cisco Unity Connection 10.x

When you install or upgrade to Cisco Unity Connection release 10.x, all objects that belong to a partition are placed in a partition named <Server Name> Partition, and all objects that are configured to use search spaces use a search space named <Server Name> Search Space (which includes <Server Name> Partition as its sole member). In addition, all templates are configured to use this partition and search space where applicable. Thus, by default, Unity Connection uses only one server-wide partition and search space. You can rename or delete the default partition and search space, and you can modify the default search space by changing the description or partition membership. (See the "Changing the System Default Partition and Search Space in Cisco Unity Connection 10.x" section on page 31-11.)

# Search Space Examples in Cisco Unity Connection 10.x

See the following sections:

- Single Site Automated Attendant Search Space Example, page 31-3
- Multiple Site Search Space Example, page 31-4

## Single Site Automated Attendant Search Space Example

CompanyA has a single Cisco Unity Connection server that is set up as an automated attendant to handle calls to the customer service department as well as handling user to user voice messages. All employees at CompanyA have a primary extension in the Employee partition. Employees who work in the customer service department also have alternate extensions in the Customer Service partition.

The Unity Connection server is configured with the following search spaces and associated partition membership:

| Search Space | Partition Membership (in Order) |
|---|---|
| Employees-SS | Employee, Customer Service |
| Customer-Service-SS | Customer Service |

In addition, the routing rules that outside callers reach are configured to use the Customer-Service-SS search space as their search scope. The system call handlers and directory handlers that outside callers interact with are configured to inherit their search scope from the call. All users use the Employees-SS as their search scope, and the routing rules that users reach when they call Unity Connection are configured to use the Employees-SS as their search space.

In this example, when users call and sign in to Unity Connection, they can address messages or place calls to any other user at the company. However, when outside callers call Unity Connection and reach the automated attendant, they can reach only those employees who have alternate extensions in the Customer Service partition.

To extend the example, CompanyA might have two operators who share the same extension: an internal operator with extension 411 in the Employee partition, and an external operator with extension 411 in the Customer Service partition. When outside callers attempt to reach extension 411, Unity Connection routes them to the external operator, because that is the only operator who appears in a partition in the

Customer-Service-SS search space. When employees call and sign in to Unity Connection and attempt to reach extension 411, Unity Connection routes them to the internal operator, because the Employee partition in which this operator extension appears is listed earlier in the partition membership of the Employees-SS search space than the Customer Service partition in which the external operator extension appears.

# Multiple Site Search Space Example

CompanyB has three digitally networked Cisco Unity Connection locations serving three sites: Headquarters, Regional-East, and Regional-West.

The configuration is as follows:

- Unity Connection is configured with the following search spaces and associated partitions:

| Search Space | Partition Membership (in Order) |
|---|---|
| Headquarters-SS | HQ, Primary, RE, RW |
| Regional-East-SS | RE, Primary |
| Regional-West-SS | RW, Primary |

- The following user accounts are set up:

| User | Home Server | Search Space of User | Primary Extension and Partition | Alternate Extension and Partition |
|---|---|---|---|---|
| Alex Abade | Headquarters | Headquarters-SS | 85553001, Primary | 3001, HQ |
| Chris Brown | Headquarters | Headquarters-SS | 85553002, Primary | 3002, HQ |
| Pat Smith | Regional-East | Regional-East-SS | 82223001, Primary | 3001, RE |
| Shannon Johnson | Regional-East | Regional-East-SS | 82223002, Primary | 3002, RE |
| Robin Smith | Regional-West | Regional-West-SS | 87773001, Primary | 3001, RW |
| Terry Jones | Regional-West | Regional-West-SS | 87773333, Primary | 3333, RW |

- There is a VPIM server that is configured as a VPIM location on the Headquarters server: VPIM-South. This VPIM location has a Dial ID of 8468 and is configured to allow blind addressing, to belong to the Primary partition, and to use the Headquarters-SS search space.
- The Attempt Sign In direct routing rule and the Attempt Forward forwarded routing rule on each server are configured to use the same search space as the users on that server. (For example, the rules on the Headquarters server use the Headquarters-SS search space.)

In this example, Unity Connection users can address other Unity Connection users at their own site by using 4-digit extensions; users can address anyone at the company by using 8 plus a 7-digit extension. Users can blind address messages to a VPIM mailbox by entering 8468 plus the mailbox number on the remote system. Messages sent by users at the VPIM-South VPIM location can be delivered to any CompanyB user in the HQ, Primary, RE, or RW partitions.

For example, if Alex Abade addresses a message by entering extension 3002 on the phone keypad, Unity Connection returns Chris Brown as the match. If Alex addresses a message by spelling SMITHR on the phone keypad (764847), Unity Connection returns both Pat Smith and Robin Smith, because both names match the 764847 spelling. If Alex addresses a message by saying "Robin Smith," Unity Connection returns Robin Smith.

The phone system can be set up to identify internal callers either by their 4-digit extension or the 8 plus 7-digit extension. Each caller must call their home server to sign in to Unity ConnectionFor information about setting up cross-server sign-in and transfers, see the "Cross-Server Sign-In, Transfers, and Live Reply in Cisco Unity Connection 10.x" chapter of the *Networking Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/networking/guide/10xcucnetx.html .)

# How Search Spaces Work in Cisco Unity Connection 10.x

See the following sections for details on the interactions between search spaces and various Unity Connection concepts:


- Search Spaces and Users, page 31-5
- Search Spaces and Call Routing Rules, page 31-6
- Search Spaces and System Distribution Lists, page 31-7
- Search Spaces and System Call Handlers, page 31-7
- Search Spaces and Directory Handlers, page 31-7
- Search Spaces and Interview Handlers, page 31-7
- Search Spaces and Networking in Cisco Unity Connection 10.x, page 31-8
- Search Spaces and VPIM Locations, page 31-8
- Search Spaces and Administrator-Defined Contacts, page 31-8


## Search Spaces and Users

When a user has signed in to Cisco Unity Connection, the search scope of the user defines the objects that the user can reach when:

- Addressing a message by extension
- Addressing a message by name
- Adding members to a private distribution list
- Adding names to an addressing priority list
- Placing a call to another user by saying the name
- Addressing a message to a VPIM contact
- Blind addressing a message to a VPIM location

Users can reach only those objects that are in a partition that is part of the search space that is defined as the search scope for the user. This search space need not include any partitions that contain the primary or alternate extensions of the user. Unity Connection applies the search scope of the user

whether the user is interacting with Unity Connection by phone (by using phone keypad keys), by using voice commands, or by using a visual client such as the Cisco Personal Communications Assistant (PCA).

If a user addresses a message by extension, and there are overlapping extensions in different partitions in the search space, Unity Connection searches the partitions in the search space in the order that they appear in the Assigned Partitions list in Cisco Unity Connection Administration, and returns the first result found.

Note that if a user receives a message from a sender whose partition is not in the search space of the receiving user, the recipient cannot reply to the sender. If the message is sent to multiple recipients, and the user replies-all, the user receives non-delivery receipts for any recipients who are not in partitions in the search space of the user (if Unity Connection is configured to send receipts)

# Search Spaces and Call Routing Rules

When a call comes in to Cisco Unity Connection, it is first checked against the applicable routing rules table, depending on whether the caller dialed directly into Unity Connection or was forwarded from an extension. When Unity Connection matches the call to a routing rule in the applicable table based on the parameters of the call, the configuration of the routing rule determines the initial search scope of the call. Other objects, such as system call handlers, may later change the search scope of the call when the call is routed to them, but the initial scope is set by the call routing rules.

To facilitate setting the correct search scope on a call routing rule, you can set up routing rule conditions to select a rule based on the port of the incoming call, the phone system, the dialed number, or other criteria. If you are setting up multiple partitions and multiple search spaces, you must carefully consider the impact of the search scope that is configured for each call routing rule. Note the following considerations related to setting the search scope with call routing rules:

- Unity Connection uses the search space defined as the initial scope of the call to identify whether the call is from a user, and if so, which user. If a user calls from an extension that is in a partition that is not a member of the search space set as the initial search scope for the call, the call is not identified as coming from the user. If the extension of the user overlaps with an extension in another partition that also appears in this search space, the call is identified as coming from the first object that Unity Connection finds when searching the partitions in the order that they appear in the search space.
- Users who call to sign in to Unity Connection do not have their search scope set to the search space defined for their user profile until they have successfully completed the sign-in process.

If users are segmented into different partitions, and extensions overlap between partitions, you must consider how Unity Connection recognizes users by extension when they call Unity Connection and attempt to sign in. For example, if Kelly Bader in Kansas City and Chris Jones in Chicago both use extension 3001, you must set up your call management plan such that when Kelly calls Unity Connection from extension 3001, Unity Connection recognizes the extension as belonging to Kelly and checks the password against the appropriate user profile; likewise when Chris calls from extension 3001. There are multiple ways to set up the routing rules to handle this. For example, you can set up a direct routing rule based on a call coming from a particular phone system, so that calls from the phone system in Kansas City match one routing rule, setting the scope of the call to a search space in which the partition that Kelly is in appears before the one that Chris is in (or the partition that Chris is in does not appear at all), and then set a similar direct routing rule for calls from Chicago. You can also set up different pilot numbers for Kansas City and Chicago, and use the Dialed Number routing rule condition to distinguish between two different routing rules that are set to use the two different search spaces.

## Search Spaces and System Distribution Lists

Because each system distribution list belongs to a partition, you can use search spaces to limit user access to send messages to lists. By placing a distribution list in a partition that is not part of the search scope of a particular group of users, these users are not able to find the distribution list to address messages to it. For example, you can create a new partition called “Distribution Lists Partition” and configure the allvoicemailusers, allvoicemailenabledcontacts, and undeliverablemessages to use this partition. To grant certain users access to send to these lists, you can create a new search space that includes both the default partition and the “Distribution Lists Partition,” and assign this search space as the search scope for those users.

## Search Spaces and System Call Handlers

Cisco Unity Connection uses the call handler search scope to match extensions that are dialed from the call handler to users, administrator-defined contacts, and remote contacts at VPIM locations. You can choose to set the scope of the handler to either inherit the search scope that is already set on the call (from a previous handler or from a call routing rule), or to use the particular search scope that you specify.

You can use call handlers to change the search scope of a call based on caller input. For example, you can set up a multiple-site automated attendant by using an introductory call handler that offers callers a menu of site choices (“Press 1 for Chicago; Press 2 for New York”). One-key dialing rules configured for this call handler send callers to either of two call handlers, which set the search scope of the call to the appropriate search space for the site (Chicago or New York) and send the call directly to the shared opening greeting call handler. After the caller makes a selection, if the caller reaches any call handlers or directory handlers that are configured to inherit the search scope of the call, these handlers are scoped correctly to reach only the users and other objects at the appropriate site.

## Search Spaces and Directory Handlers

You can configure the scope of a directory handler to define the objects that callers who reach the directory handler can find or hear. For phone directory handlers, you can set the scope to the entire server, to a particular class of service, to a system distribution list, or to a search space (either inherited from the call or specified for the directory handler). For voice-enabled directory handlers, you can set the scope to the entire server or to a search space (either inherited from the call or specified for the directory handler).

When callers search a directory handler for a particular name, if the scope of the directory handler is set to a search space, Cisco Unity Connection searches each partition in the search space and returns a list of all of the objects that match the name.

## Search Spaces and Interview Handlers

Each interview handler is associated with a partition, so that it can be included in a search space and callers can reach it from other parts of the conversation. Because interview handlers do not involve dialing or addressing to users or other objects, they do not have a search scope defined.

# Search Spaces and Networking in Cisco Unity Connection 10.x

When you network a Cisco Unity Connection server with other Unity Connection locations, the partitions and search spaces that are configured on the server replicate to all other Unity Connection locations on the network. A Unity Connection network supports up to 10K partitions and 10K search spaces shared among all of the locations in the network.

If you plan to connect multiple Unity Connection servers in a network, it is important to note that when you initially set up the network between the servers, users on one server are not able to address messages to users on other servers, because the users on each server are in separate partitions and use search spaces that do not contain partitions with users on the other server. At a minimum, to allow users to address to users on other servers, you must add the partition of the remote Unity Connection server to the search space that local users are using.

# Search Spaces and VPIM Locations

Each VPIM location belongs to a single partition. If a VPIM location allows blind addressing, and the partition to which the location belongs is in the search space for a user, the user can blind address to a user on the remote VPIM system. To blind address, the user addresses the message to the Dial ID of the VPIM location followed by the remote user mailbox number. For example, to reach mailbox 1000 at VPIM location 555, the user would address the message to 5551000.

The partition of the VPIM location is used as the partition of automatically-created VPIM contacts if the VPIM location is configured for automatic contact creation. However, you can change the partition of VPIM contacts independent of the associated VPIM location in Cisco Unity Connection Administration. A Unity Connection user can address a message to a VPIM contact by spelling or saying the contact name or by saying “<Name> at <Location>” provided that the contact belongs to a partition that is in the search space of the Unity Connection user.

Each VPIM location also has a search scope. When Unity Connection receives a message from a sender at a VPIM location, Unity Connection searches the search space that is defined as the search scope for the location to determine the message recipient by matching the extension in the To: address field with a Unity Connection user.

Note that when users address messages to a VPIM mailbox by entering a VPIM location Dial ID plus a remote user mailbox number, or when voice-recognition users say a name and location (for example, “John Smith in Seattle”), the action is allowed or denied based on the partition of the VPIM location. However, when users address to a VPIM contact by using spell-by-name or by entering the local extension of the contact, or when voice-recognition users say the name of a contact without the location (for example, “John Smith”), the action is allowed or denied based on the partition of the VPIM contact, regardless of whether the partition of the VPIM location is out of scope for the user.

# Search Spaces and Administrator-Defined Contacts

Each administrator-defined contact belongs to a partition. When a contact is configured with phone numbers that callers can use to call the contact by using voice commands, voice-recognition users whose search space includes the partition of the contact are able to call the contact; users whose search space does not include this partition are not able to call the contact. In addition, the contact is reachable by callers who reach any voice-enabled directory handler whose search scope uses or inherits a search space that includes this partition (or if the directory handler search scope is set to the entire server).

# Managing Partitions in Cisco Unity Connection 10.x

You create a partition in Cisco Unity Connection Administration by naming the partition and saving it. When you have created the partition, you populate it by configuring individual objects or templates as partition members.

### To Create a Partition

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Partitions**.

**Step 2** On the **Search Partitions** page, select **Add New**.

**Step 3** On the **New Partition** page, enter a name for the partition.

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

**Step 5** On the **Edit Partition** page, you can add a description for the partition to describe its use or to distinguish it from other partitions. To do so, enter text in the **Description** field and select **Save**.

You can change the name or description of a partition. To change the partition membership, you must edit the individual member objects.

### To Modify a Partition

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Partitions**.

**Step 2** On the **Search Partitions** page, select the display name of the partition that you want to modify.

**Note** If the partition that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Partition** page, change the name or description, as applicable.

**Step 4** When you have finished changing settings on the **Edit Partition** page, select **Save**.

You can delete a partition when the partition is empty (there are no objects that are members of the partition) and when the partition is not configured as the system default partition. If you attempt to delete a partition that is not empty, Cisco Unity Connection warns you that the partition is in use, and does not allow the deletion.

### To Delete a Partition

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Partitions**.

**Step 2** On the **Search Partitions** page, check the check box next to the display name of the partition that you want to delete.

**Note** If the partition that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** Select **Delete Selected**, and select **OK** to confirm the deletion.

# Managing Search Spaces in Cisco Unity Connection 10.x

### To Create a Search Space

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Search Spaces**.

**Step 2** On the **Search Spaces** page, select **Add New**.

**Step 3** On the New Search Space page, enter a name for the search space.

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

**Step 5** On the **Edit Search Space** page, enter a description for the search space.

**Step 6** To add a partition to the list of partitions that are assigned to the search space, select the name of the partition in the **Unassigned Partitions** list, then select the **Up** arrow above the list.

**Step 7** To change the order of partitions in the **Assigned Partitions** list, select the name of the partition to move, then select the **Up** or **Down** arrow to the right of the list.

**Step 8** When you are done modifying the partition membership, select **Save**.

### To Modify a Search Space

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Search Spaces**.

**Step 2** On the **Search Spaces** page, select the display name of the search space that you want to modify.

**Step 3** On the **Edit Search Space** page, change settings as applicable.

**Step 4** To add a partition to the list of partitions that are assigned to the search space, select the name of the partition in the **Unassigned Partitions** list, then select the **Up** arrow above the list.

**Step 5** To change the order of partitions in the **Assigned Partitions** list, select the name of the partition to move, then select the **Up** or **Down** arrow to the right of the list.

**Step 6** When you have finished changing settings on the **Edit Search Space** page, select **Save**.

You can delete a search space even when there are objects using it; however, in this case you must choose a replacement search space. Objects that had a search scope set to the deleted search space are changed to use the replacement search space instead.

### To Delete a Search Space

**Step 1** In Cisco Unity Connection Administration, expand **Dial Plan**, then select **Search Spaces**.

**Step 2** On the **Search Spaces** page, check the check box next to the display name of the search space that you want to delete.

**Note** If the search space that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** Select **Delete Selected**, and select **OK** to confirm the deletion.

**Note** You cannot delete more than 50 search spaces simultaneously.

# Changing the System Default Partition and Search Space in Cisco Unity Connection 10.x

The system default partition and search space are used when you create new objects that are not based on templates (for example, a new call handler template, directory handler, or interview handler; or a new routing rule). The system default partition is displayed by default in any Partition list for such new objects in Cisco Unity Connection Administration, and the system default search space is displayed by default in any Search Scope list; these values are used when the object is created unless the administrator selects a different value from the list before saving the page. They can also be changed later by editing the object.

**Note** Changing the system default partition and search space does not affect any objects or templates that have already been created.

### To Change the System Default Partition and Search Space

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **General Configuration**.

**Step 2** On the **Edit General Configuration** page, in the **Default Partition** field, select the name of the new default partition.

**Step 3** In the **Default Search Scope** field, select the name of the new default search space.

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

# Finding Objects that Belong to a Partition or Search Space in Cisco Unity Connection 10.x

There are several methods available for locating objects based on the partition or search space to which they belong. See the following sections:

- Finding Objects Based on Partition in Cisco Unity Connection Administration, page 31-12
- Finding Users Based on Partition in Cisco Unity Connection Serviceability, page 31-12

# Finding Objects Based on Partition in Cisco Unity Connection Administration

In Cisco Unity Connection Administration, you can use the **Search Limits** fields on the search pages for the objects that have partition membership to locate the objects of that type that belong to a particular partition.

Use the following procedure to limit a search by partition.

### To Limit a Search by Partition

**Step 1** In Cisco Unity Connection Administration, go to the applicable **Search** page.

**Step 2** In the **Limit Search To** list, select **Partition**.

**Step 3** In the **Where Name Is** list, select the name of the partition in which to find objects.

**Note** When searching for users, you can also select whether to display only the primary extension in the partition, or both the primary extension and any alternate extensions that appear in the partition. If you select to display both the primary extension and any alternate extensions, multiple records may display for a single user in the search results.

**Step 4** Optionally, to further limit the search, in the search fields, indicate the search parameters, and enter the applicable characters to search for. Select **Find**.

# Finding Users Based on Partition in Cisco Unity Connection Serviceability

You can use the **Dial Search Scope** report in Cisco Unity Connection Serviceability to get a list of all users who are members of each search space in the Cisco Unity Connection directory. For each search space, the report lists each partition in the search space, and for each partition, the report lists each user and the corresponding user extension (primary or alternate) that is in the partition.

For more information on generating and viewing reports, see the *Administration Guide for Cisco Unity Connection Serviceability Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/serv_administration/guide/10xcucservagx.html.

# Managing the Phone System Integrations in Cisco Unity Connection 10.x

**Note** You can manage the phone system integrations by adding or deleting phone systems, port groups, ports, phone system trunks, and servers. You can also change the settings for existing phone systems, port groups, ports, phone system trunks, and servers.

See the following sections:


- Managing Phone Systems in Cisco Unity Connection 10.x, page 32-1
- Managing Port Groups in Cisco Unity Connection 10.x, page 32-7
- Managing Ports in Cisco Unity Connection 10.x, page 32-18
- Managing Speech Connect Port in Cisco Unity Connection 10.x, page 32-21
- Managing Phone System Trunks in Cisco Unity Connection 10.x, page 32-22
- Security in Cisco Unity Connection 10.x (Cisco Unified Communications Manager Integrations Only), page 32-23
- IPv6 in Cisco Unity Connection (Cisco Unified Communications Manager Integrations Only), page 32-27


## Managing Phone Systems in Cisco Unity Connection 10.x

The phone system pages in Cisco Unity Connection Administration identify the phone systems that Cisco Unity Connection integrates with. In Connection Administration, a phone system has one or more port groups, which in turn have voice messaging ports. You can manage the phone systems to meet the changing needs of your system.

See the following sections:


- Adding a New Phone System Integration, page 32-2
- Deleting a Phone System Integration, page 32-2
- Changing Phone System Settings, page 32-3
- Listing the Users Who Are Associated with the Phone System, page 32-3
- Disabling the Use of the Same Port for Turning On and Off an MWI, page 32-4
- Synchronizing MWIs for the Phone System, page 32-4

- Configuring Phone View Settings (Cisco Unified Communications Manager Integrations Only), page 32-4
- Changing Call Loop Detection Settings, page 32-5
- Managing AXL Servers, page 32-5

# Adding a New Phone System Integration

You can integrate multiple phone systems with Cisco Unity Connection. For a matrix of supported combinations, see the *Multiple Integration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support adding new phone system integrations.

### To Add a New Phone System Integration

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, under **Phone System Search Results**, select **Add New**. The **New Phone System** page appears.

**Step 3** On the **New Phone System** page, in the **Phone System Name** field, enter a descriptive name for the phone system and select **Save**.

**Step 4** On the **Phone System Basics** page, enter the applicable settings and select **Save**.

# Deleting a Phone System Integration

You can delete a phone system when the phone system is no longer used by Cisco Unity Connection. Before you can delete a phone system, you must delete or reassign to another phone system all of the following objects that are associated with the phone system that you want to delete:

- All users (including MWI devices and notification devices)
- All user templates
- All system call handlers
- All call handler templates

**Note** You can see a list of all users who are associated with the phone system on the Phone System Associations page. For instructions, see the "Listing the Users Who Are Associated with the Phone System" section on page 32-3.
Cisco Unified Communications Manager Business Edition (CMBE) does not support deleting a phone system integration.

### To Delete a Phone System Integration

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, under **Phone System Search Results**, check the check box next to the name of the phone systems that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the phone systems, select **OK**.

## Changing Phone System Settings

You can change the settings for a phone system after it is integrated with Cisco Unity Connection. The phone system settings identify the phone system that Unity Connection integrates with and regulate certain phone system features. (Integration configuration settings are located in the port groups that belong to the phone system.)

### To Change Phone System Settings

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system for which you want to change the settings.

**Step 3** On the **Phone System Basics** page, change the applicable settings and select **Save**.

## Listing the Users Who Are Associated with the Phone System

You can view a list of all of the Cisco Unity Connection users who are associated with the phone system.

### To List the Users Who Are Associated with the Phone System

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system.

**Step 3** On the **Phone System Basics** page, on the **Edit** menu, select **Phone System Associations**.

**Step 4** On the **Phone System Associations** page, the list of users who are associated with the phone system is displayed.

# Disabling the Use of the Same Port for Turning On and Off an MWI

If you created the phone system integration to use the same voice messaging port to turn on and off an MWI (the Use Same Port for Enabling and Disabling MWIs field was checked), you can do the following procedure to disable this configuration without leaving MWIs on when there are no voice messages for the user.

### To Disable the Use of the Same Port for Turning On and Off an MWI

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system.

**Step 3** On the **Phone System Basics** page, check the **Force All MWIs Off for This Phone System** check box and select **Save**.

**Step 4** Uncheck the **Use Same Port for Enabling and Disabling MWIs** and the **Force All MWIs Off for This Phone System** check boxes, then select **Save**.

**Step 5** Select **Run** in front of **Synchronize All MWIs on This Phone System**.

# Synchronizing MWIs for the Phone System

You can synchronize all message waiting indicators (MWIs) for a phone system without affecting MWIs on other phone systems.

### To Synchronize MWIs for the Phone System

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system.

**Step 3** On the **Phone System Basics** page, select **Run** in front of **Synchronize All MWIs on This Phone System**.

# Configuring Phone View Settings (Cisco Unified Communications Manager Integrations Only)

For Cisco Unified Communications Manager integrations, Phone View allows users to see search results on the LCD screens of their Cisco IP phones when they use the Find Message or the Display Message menu. Phone View requires that Cisco Unified CM also be configured. For details, see the "Setting Up Phone View in Cisco Unity Connection 10.x" chapter.

### To Configure Phone View Settings (Cisco Unified Communications Manager Integrations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system.

**Step 3** On the **Phone System Basics** page, under **Phone View Settings**, enter the applicable settings and select **Save**.

# Changing Call Loop Detection Settings

Calls that Cisco Unity Connection forwards (for example, to notify a user that a message has been received) are sometimes forwarded back to Unity Connection. When call loop detection is enabled, Unity Connection detects when a call loop has occurred and rejects the call.

You can change the call loop detection settings to enable or disable the types of calls that are checked, to set the fourth-column DTMF tone that Unity Connection uses, and to set the guard time.

The call loop detection settings should not be changed without understanding the effect that they have on calls that Unity Connection forwards.

### To Change Call Loop Detection Settings

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the phone system.

**Step 3** On the **Phone System Basics** page, under **Call Loop Detection by Using DTMF**, enter applicable settings and select **Save**.

# Managing AXL Servers

AXL servers are supported only for Cisco Unified Communications Manager phone systems and are 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 Unity Connection personal call transfer rules.

AXL servers are not supported for Cisco Unified Communications Manager Express integrations.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support adding AXL servers. Adding AXL servers is not needed for Cisco Unified CMBE.
When a Unity Connection cluster is configured, you must be signed in to the publisher server of the Unity Connection cluster to import Cisco Unified CM user data.

See the following procedures:

- To Add AXL Servers, page 32-5
- To Delete an AXL Server, page 32-7
- To Change AXL Server Settings, page 32-7

### To Add AXL Servers

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the Cisco Unified CM phone system.

**Step 3** On the **Phone System Basics** page, on the **Edit** menu, select **Cisco Unified Communications Manager AXL Servers**.

**Step 4** On the **Edit AXL Servers** page, under AXL Servers, select **Add New**.

**Step 5** Enter the following settings for the AXL server and select **Save**.

*Table 32-1 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.<br>For Cisco Unified Communications Manager version 4.1(x), the port number is typically 443.<br>For Cisco Unified Communications Manager version 5.x or later, the port number is typically 8443. |

**Step 6** Repeat Step 4 and Step 5 for all remaining AXL servers that you want to add.

**Step 7** Under AXL Server Settings, enter the following settings and select **Save**.

*Table 32-2 Settings for the AXL Server Settings*

| Field | Setting |
|---|---|
| User Name | Enter the username that Unity Connection uses to sign in to the AXL server.<br>**Note** This user must match the username 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.<br>**Note** This password must match the password of the Cisco Unified CM application user entered in the User Name field. |

**Step 8** To add a corresponding application server to Cisco Unified CM, sign in to Cisco Unified CM Administration.

**Step 9** In Cisco Unified CM Administration, go to the **System > Application Server** page.

**Step 10** On the **Find and List Application Servers** page, select **Find** to display all application servers.

**Step 11** In the **Name** column, select the name of the Cisco Unity Connection server.

**Step 12** On the **Application Server Configuration** page, in the **Available Application User** field, select the Cisco Unified CM application user that you used in Step 7 and select the **Down** arrow to move it to the **Selected Application User** field.

**Step 13** Select **Save**.

### To Delete an AXL Server

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the Cisco Unified CM phone system.

**Step 3** On the **Phone System Basics** page, on the **Edit** menu, select **Cisco Unified Communications Manager AXL Servers**.

**Step 4** On the **Edit AXL Servers** page, under AXL Servers, check the check box next to the AXL server that you want to delete.

**Step 5** Select **Delete Selected**.

**Step 6** When prompted to confirm that you want to delete the AXL server, select **OK**.

### To Change AXL Server Settings

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** On the **Search Phone Systems** page, select the display name of the Cisco Unified CM phone system.

**Step 3** On the **Phone System Basics** page, on the **Edit** menu, select **Cisco Unified Communications Manager AXL Servers**.

**Step 4** On the **Edit AXL Servers** page, change the applicable settings and select **Save**.

# Managing Port Groups in Cisco Unity Connection 10.x

Port groups hold most of the integration configuration settings and some or all of the voice messaging ports for Cisco Unity Connection.

While most phone system integrations need only one port group, multiple port groups may be needed in the following circumstances:

- For integrations with phone systems through PIMG/TIMG units, each PIMG/TIMG unit is connected to one port group with the applicable voice messaging ports. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit.
- For integrations with other phone systems, an additional port group with its own voice messaging ports may be used for testing a new configuration or for troubleshooting.

Unity Connection port groups provide flexibility for integration configuration settings that apply to different sets of ports.

See the following sections:

- Adding a Port Group, page 32-8
- Deleting a Port Group, page 32-8
- Changing Port Group Settings, page 32-9
- Changing the Audio Format That Cisco Unity Connection Uses for Calls, page 32-9
- Changing MWI Settings, page 32-11
- Adding Secondary Cisco Unified Communications Manager Servers, page 32-11

- Deleting Cisco Unified Communications Manager Servers, page 32-12
- Changing Cisco Unified Communications Manager Server Settings, page 32-12
- Adding a TFTP Server, page 32-13
- Deleting a TFTP Server, page 32-13
- Changing TFTP Server Settings, page 32-14
- Adding a SIP Server, page 32-14
- Deleting a SIP Server, page 32-15
- Changing SIP Server Settings, page 32-15
- Managing PIMG/TIMG Units, page 32-16
- Changing Session Initiation Protocol (SIP) Settings, page 32-17
- Changing Port Group Advanced Settings, page 32-17
- Enabling or Disabling Normalization, page 32-17


# Adding a Port Group

You can add multiple port groups, each with its own integration configuration settings and its own voice messaging ports. In Unity Connection 10.0(1), in case of video calls, only SIP integration mode is supported.

*Cisco Unified Communications Manager Business Edition (CMBE) only:* Before you can add a port group, you must have existing voice messaging ports in Cisco Unified CM Administration that do not belong to a port group.

*Other configurations:* For integrations with phone systems through PIMG/TIMG units, one port group is required for each PIMG/TIMG unit. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit.

**Note** Cisco Unity Connection enables you to create a maximum of 90 port groups if you are using only TUI (touchtone conversation) and VUI (voice-recognition) features of Cisco Unity Connection. However, if you are using all the features of Unity Connection, you are allowed to create a maximum of 60 port groups.

### To Add a Port Group

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

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

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

# Deleting a Port Group

When you delete a port group, any voice messaging ports that belong to it are deleted at the same time, but the phone system that the port group belongs to is not deleted.

### To Delete a Port Group

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

**Step 2** On the **Search Port Groups** page, under **Port Group Search Results**, check the check box next to the port group name of the port groups that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the port group, select **OK**.

## Changing Port Group Settings

You can change the settings for a port group after it has been added. Changes to the settings affect only the voice messaging ports that belong to the port group.

### To Change Port Group Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change the settings.

**Step 3** On the **Port Group Basics** page, change the applicable settings and select **Save**.

## Changing the Audio Format That Cisco Unity Connection Uses for Calls

For calls, Cisco Unity Connection advertises the audio format (or codec) that is preferred for the media stream with the phone system. You should consider the following when setting the audio format:

- For the following reasons, Unity Connection should use the same audio format for the media stream that the phone system uses:
  - To reduce the need for transcoding the media stream from one audio format to another.
  - To minimize the performance impact on the Unity Connection server and on the phone system.
  - To preserve the audio quality of calls.
- When Unity Connection advertises a different audio format than the one used by the phone system, the phone system transcodes the media stream.

### To Change the Audio Format That Cisco Unity Connection Uses for Calls

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

**Step 2** On the **Search Port Groups** page, select the first port group that belongs to the phone system integration for which you want to change the audio format of the media stream.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Codec Advertising**.

**Step 4** On the **Edit Codec Advertising** page, select the **Up** and **Down** arrows to change the order of the codecs or to move codecs between the **Advertised Codec** box and the **Unadvertised Codecs** box.

If only one codec is in the **Advertised Codecs** box, Cisco Unity Connection sends the media stream in that audio format. The phone system transcodes if it does not use this audio format.

If two or more codecs are in the **Advertised Codecs** box, Unity Connection advertises its preference for the first codec in the list but sends the media stream in the audio format from the list that the phone system selects.

**Step 5** Select **Save**.

**Step 6** *(All integrations except SCCP)* If you want to change the packet size that is used by the advertised codecs, on the **Port Group Basics** page, under **Advertised Codec Settings,** select the applicable packet setting for each codec and select **Save**.

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

**Step 8** Repeat Step 3 through Step 7 for all remaining port groups that belong to the phone system integration for which you want to change the audio format of the media stream.

# Changing the Video Format that Cisco Unity Connection 10.x Uses for Calls

For calls, Cisco Unity Connection advertises the video format (or codec) that is preferred for the media stream with the phone system. You should consider the following when setting the video format:

- When Unity Connection advertises a different video format than the one used by the phone system, the phone system transcodes the media stream.
- Unity Connection should use the same video format for the media stream that the phone system uses for the following reasons:
  - To reduce the need for transcoding the media stream from one video format to another.
  - To minimize the performance impact on the Unity Connection server and on the phone system.
  - To preserve the video quality of calls.

**Note** In Cisco Unity Connection 10.0(1), only G.711 mu-law video format (or codec) is supported to record and play video greetings.

For more information on video format codecs, see the "Video Codecs" section in the ""Sizing and Scaling Cisco Unity Connection 10.x Servers" chapter of the *Design Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html.

### To Change the video Format That Cisco Unity Connection Uses for Calls

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

**Step 2** On the **Search Port Groups** page, select the port group that belongs to the phone system integration for which you want to change the video format of the media stream.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Codec Advertising**.

**Step 4** On the **Edit Codec Advertising** page, select the **Up** and **Down** arrows to move the G.711 mu-law codec between the **Advertised Codec** box and the **Unadvertised Codecs** box.

If only one codec is in the **Advertised Codecs** box, Cisco Unity Connection sends the media stream in that video format. The phone system transcodes if it does not use this video format.

**Step 5** Select **Save**.

**Step 6** *(Only SIP integrations)* If you want to change the packet size that is used by the advertised codecs, on the **Port Group Basics** page, under **Advertised Codec Settings**, select the applicable packet setting for each codec in the **Packet Size** list, and select **Save**.

**Step 7** On the **Port Group** menu, select **Search Port Groups**.

**Step 8** Repeat Step 2 through Step 7 for all remaining port groups that belong to the phone system integration for which you want to change the video format of the media stream.

# Changing MWI Settings

Messaging waiting indicators (MWIs) control whether Cisco Unity Connection sets MWIs for users and how retries for MWI requests are handled.

### To Change MWI Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change the MWI settings.

**Step 3** On the **Port Group Basics** page, under **Message Waiting Indicator Settings,** change the applicable settings and select **Save**.

# Adding Secondary Cisco Unified Communications Manager Servers

For Cisco Unified Communications Manager integrations, Related Links helps you create the integration only with one Cisco Unified CM server. The secondary Cisco Unified CM servers in the cluster must be added after the integration is created.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support secondary Cisco Unified CM servers.

### To Add Secondary Cisco Unified Communications Manager Servers

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to add secondary 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 Servers**, select **Add**.

**Step 5** Enter the settings for the secondary Cisco Unified CM server and select **Save**.

**Step 6** Repeat Step 4 and Step 5 for all remaining secondary Cisco Unified CM servers that you want to add.

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

# Deleting Cisco Unified Communications Manager Servers

You can delete a Cisco Unified Communications Manager server when it is no longer used by the phone system integration.

If you want to move a Cisco Unified CM server to another port group, you must delete the Cisco Unified CM server from one port group and add it to the second port group.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support deleting Cisco Unified CM servers.

### To Delete a Cisco Unified Communications Manager Server

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to delete 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 Servers, check the check box next to the Cisco Unified CM servers that you want to delete.

**Step 5** Select **Delete Selected**.

**Step 6** When prompted to confirm that you want to delete the Cisco Unified CM servers, select **OK**.

# Changing Cisco Unified Communications Manager Server Settings

You can change the Cisco Unified CM server settings after the server has been added.

### To Change Cisco Unified Communications Manager Server Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change Cisco Unified CM server settings.

**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 Servers,** change the applicable settings and select **Save**.

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

# Adding a TFTP Server

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

If your system uses authentication and encryption for the Unity Connection voice messaging ports, you must add a TFTP server after you create the Cisco Unified CM phone system integration.

### To Add a TFTP Server

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to add a TFTP server.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under TFTP Servers, select **Add**.

**Step 5** Enter the settings for the TFTP server and select **Save**.

**Step 6** Repeat Step 4 and Step 5 for all remaining TFTP servers that you want to add.

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

# Deleting a TFTP Server

You can delete a TFTP server when it is no longer used by the port group.

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

### To Delete a TFTP Server

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to delete a TFTP server.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under TFTP Servers, check the check box next to the TFTP server that you want to delete.

**Step 5** Select **Delete Selected**.

**Step 6** When prompted to confirm that you want to delete the TFTP server, select **OK**.

# Changing TFTP Server Settings

You can change the TFTP server settings after the server has been added.

For Cisco Unified Communications Manager integrations, TFTP servers are required only when the Cisco Unified CM cluster uses authentication and encryption for the Cisco Unity Connection voice messaging ports.

### To Change TFTP Server Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change TFTP server settings.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under TFTP Servers, change the applicable settings and select **Save**.

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

# Adding a SIP Server

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can add another SIP server after the phone system has been created.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

### To Add a SIP Server

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to add SIP servers.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under SIP Servers, select **Add**.

**Step 5** Enter the settings for the SIP server and select **Save**.

**Step 6** Repeat Step 4 and Step 5 for all remaining SIP servers that you want to add.

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

# Deleting a SIP Server

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can delete a SIP server when it is no longer used by the port group.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

### To Delete a SIP Server

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to delete SIP servers.

**Step 3** On the **Port Group Basics** page, on the Edit menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under SIP Servers, check the check box next to the SIP server that you want to delete.

**Step 5** Select **Delete Selected**.

**Step 6** When prompted to confirm that you want to delete the SIP server, select **OK**.

# Changing SIP Server Settings

For a phone system integration with Cisco Unified Communications Manager through a SIP trunk or with another SIP server, you can change the SIP server settings after the server has been added.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support SIP servers.

### To Change SIP Server Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change SIP server settings.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Servers**.

**Step 4** On the **Edit Servers** page, under **SIP Servers,** change the applicable settings and select **Save**.

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

# Managing PIMG/TIMG Units

For integrations with phone systems through PIMG/TIMG units, each PIMG/TIMG unit is in a separate port group. For example, a system that uses five PIMG units requires five port groups, one port group for each PIMG unit. You can add, change, or delete PIMG/TIMG units after the phone system integration has been created.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support integrations with PIMG/TIMG units.

See the following procedures:

- To Add PIMG/TIMG Units, page 32-16
- To Delete PIMG/TIMG Units, page 32-16
- To Change PIMG/TIMG Settings, page 32-16

### To Add PIMG/TIMG Units

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

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

**Step 3** On the **New Port Group** page, in the **Phone System** field, select the phone system for which you want to add a PIMG/TIMG unit.

**Step 4** Enter the applicable settings and select **Save**.

### To Delete PIMG/TIMG Units

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

**Step 2** On the **Search Port Groups** page, under **Port Group Search Results**, check the check box next to the port group for the PIMG/TIMG unit that you want to delete.

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

### To Change PIMG/TIMG Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change PIMG/TIMG settings.

**Step 3** On the **Port Group Basics** page, under **PIMG Settings**, change the applicable settings and select **Save**.

# Changing Session Initiation Protocol (SIP) Settings

For integrations that use session initiation protocol (SIP), you can change the SIP settings after the phone system integration has been created.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support integrations that use SIP.

### To Change Session Initiation Protocol (SIP) Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change SIP settings.

**Step 3** On the **Port Group Basics** page, under **Session Initiation Protocol (SIP) Settings**, change the applicable settings and select **Save**.

# Changing Port Group Advanced Settings

The port group advanced settings control infrequently used settings such as delays and MWI usage. We recommend that port group advanced settings be left at their default values.

### To Change Port Group Advanced Settings

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change the advanced settings.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Advanced Settings**.

**Step 4** On the **Edit Advanced Settings** page, under **Port Group Advanced Settings,** change the applicable settings and select **Save**.

# Enabling or Disabling Normalization

Normalization controls automatic volume adjustments for recording messages. We recommend that you leave normalization enabled and that you not change the value of the **Target Decibel Level for Recordings and Messages** field on the **System Settings > General Configuration** page.

### To Enable or Disable Normalization

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

**Step 2** On the **Search Port Groups** page, select the display name of the port group for which you want to change the advanced settings.

**Step 3** On the **Port Group Basics** page, on the **Edit** menu, select **Advanced Settings**.

**Step 4** On the **Edit Advanced Settings** page, under **Audio Normalization for Recordings and Messages**, change the applicable settings and select **Save**.

# Managing Ports in Cisco Unity Connection 10.x

The voice messaging ports let Cisco Unity Connection receive calls (for example, to record a message) and let Unity Connection make calls (for example to send message notifications or to set MWIs).

Each voice messaging port can belong to only one port group. Port groups, when there are several, each have their own voice messaging ports. The total voice messaging ports belonging to all port groups must not exceed the maximum number of voice messaging ports that are enabled by the Unity Connection license files.

See the following sections:


- Adding a Port, page 32-18
- Deleting a Port, page 32-19
- Changing Port Settings, page 32-19
- Viewing the Port Certificate, page 32-21


## Adding a Port

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system. You can add voice messaging ports after the phone system has been created. The number of voice messaging ports that you add cannot bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the Unity Connection license files.

*Cisco Unified Communications Manager Business Edition (CMBE) only:* Before you can add ports, you must have existing voice messaging ports in Cisco Unified CM Administration that do not belong to a port group.

### To Add a New Port

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

**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**.

**Caution** Verify 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 may not function correctly. See the "Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection" section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

**Step 4** In Cisco Unity Connection Administration, in the **Related Links** list, select **Check Telephony Configuration** and select **Go** to confirm the phone system integration settings.

**Step 5** If the test is not successful, the **Task Execution Results** list displays one or more messages with troubleshooting steps. After correcting the problems, check the configuration again.

# Deleting a Port

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system.

### To Delete a Port

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

**Step 2** On the **Search Ports** page, under **Port Search Results**, check the check box 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.

# Changing Port Settings

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system. You can change the voice messaging port settings after the phone system integration has been created.

### To Change Port Settings

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

**Step 2** On the **Search Ports** page, select the display name of the voice messaging port for which you want to change the settings.

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

Depending on the phone system integration, some or all of the fields in Table 32-3 appear.

*Table 32-3 Port Basics Page Settings*

| Field | Considerations |
|---|---|
| Enabled | Check this check box to enable the port. The port is enabled during normal operation.<br>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. |

*Table 32-3 Port Basics Page Settings (continued)*

| Field | Considerations |
|---|---|
| Server Name<br>*(not available for PIMG/TIMG integrations)* | *(For Cisco Unity Connection redundancy only)* Select the name of the Cisco Unity Connection server that you want to handle this port.<br>Assign an equal number of answering and dial-out voice messaging ports to the Unity Connection servers so that they equally share the voice messaging traffic. |
| Extension<br>*(available for PIMG/TIMG integrations only)* | Enter the extension for the port as assigned on the phone system. |
| Answer Calls | Check this check box to designate the port for answering calls. These calls can be incoming calls from outside callers or from users. |
| Perform Message Notification | Check this check box to designate the port for notifying users of messages. Assign Perform Message Notification to the least busy ports. |
| Send MWI Requests<br>*(not used by serial integrations)* | Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports.<br>For serial integrations, uncheck this check box. Otherwise, the integration may not function correctly. |
| Allow TRAP Connections | Check this check box so that users can use the port for recording and playback through the phone in Cisco Unity Connection web applications. Assign Allow TRAP Connections to the least busy ports. |
| Outgoing Hunt Order<br>*(not available for SIP integrations)* | Enter the priority order in which Cisco Unity Connection uses 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 uses the port that has been idle the longest. |
| Security Mode<br>*(available for Cisco Unified CM SCCP integrations only)* | Select the applicable security mode:<br>• **Non-secure**—The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text and are connected to Cisco Unified Communications Manager through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream is not encrypted.<br>• **Authenticated**—The integrity of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages are not ensured because they are sent as clear (unencrypted) text. In addition, the media stream are not encrypted.<br>• **Encrypted**—The integrity and privacy of call-signaling messages are 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. |

**Step 4** If there are no more voice messaging ports for which you want to change the settings, skip to Step 6. Otherwise, select **Next**.

**Step 5** Repeat Step 3 and Step 4 for all remaining voice messaging ports for which you want to change the settings.

**Step 6** On the **Port** menu, select **Search Ports**.

**Step 7** On the **Search Ports** page, confirm 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. If necessary, adjust the number of voice messaging ports set to answer calls and an appropriate number of voice messaging ports set to dial out.

## Viewing the Port Certificate

Port certificates for voice messaging ports are used only by SCCP integrations with Cisco Unified Communications Manager 4.1 and later, and are required for authentication of the Cisco Unity Connection voice messaging ports. You can view the port certificate to help in troubleshooting authentication and encryption problems.

### To View the Port Certificate

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

**Step 2** On the **Search Ports** page, select the display name of the voice messaging port for which you want to see the device certificate.

**Step 3** On the **Port Basics** page, select **View Certificate**.

**Step 4** In the **View Port Certificate** window, the information from the port device certificate is displayed.

# Managing Speech Connect Port in Cisco Unity Connection 10.x

Speech Connect uses voice-enabled directory handlers that allow both employees and outside callers to speak the name of an employee and instantly get connected, without having to navigate an audio-text tree, and without knowing the extension of the employee. For easy access, you can configure a Speech Connect speed dial on user phones.

See the following sections:

- Configuring a Speech Connect Port, page 32-21

## Configuring a Speech Connect Port

### To Configure a New Speech Connect Port

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Speech Connect Port**.

**Step 2** On the **Speech Connect Port** page, under **New Speech Connect Port**, select the Unity Connection server from the Unity Connection **Server** drop down list.

**Step 3** In the **Number of Ports** field, enter the number of Speech Connect ports that you want to configure.

**Step 4** Click on the **Save** option to apply the specified settings.

# Managing Phone System Trunks in Cisco Unity Connection 10.x

When multiple phone systems are integrated with Cisco Unity Connection, you may want to set up a phone system trunk so that calls on one phone system can be transferred to extensions on another phone system. Phone system trunks are accessed by dialing extra digits (for example, dialing 9) before dialing the extension.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

See the following sections:

- Adding a Phone System Trunk, page 32-22
- Deleting a Phone System Trunk, page 32-22
- Changing Phone System Trunk Settings, page 32-23

## Adding a Phone System Trunk

If another phone system integration exists, you can add a phone system trunk to provide access from calls on one phone system to extensions on the other phone system. You can add phone system trunks after the phone system integration has been created.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

### To Add a Phone System Trunk

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**.

**Step 2** On the **Search Phone System Trunks** page, under **Phone System Trunk Search Results**, select **Add New**.

**Step 3** On the **New Phone System Trunk** page, enter the applicable settings and select **Save**.

## Deleting a Phone System Trunk

You can delete a phone system trunk when it is no longer used by a phone system integration.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

### To Delete a Phone System Trunk

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**.

**Step 2** On the **Search Phone System Trunks** page, under **Phone System Trunk Search Results**, check the check box next to the phone system trunk that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the phone system trunk, select **OK**.

## Changing Phone System Trunk Settings

Phone system trunk settings cannot be changed. However, you can delete the phone system trunk that you want to change and add a new phone system trunk with the settings that you want.

**Note** Cisco Unified Communications Manager Business Edition (CMBE) does not support phone system trunks.

### To Change Phone System Trunk Settings

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**.

**Step 2** On the **Search Phone System Trunks** page, check the check box next to the phone system trunk that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the phone system trunk, select **OK**.

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

**Step 6** On the **New Phone System Trunk** page, enter the applicable settings and select **Save**.

# Security in Cisco Unity Connection 10.x (Cisco Unified Communications Manager Integrations Only)

When Cisco Unified Communications Manager authentication and encryption is configured for Cisco Unity Connection voice messaging ports, you can manage certifications and the security profile.

See the following sections:

- Viewing the Cisco Unity Connection Root Certificate, page 32-24
- Saving the Cisco Unity Connection Root Certificate as a File, page 32-24
- Adding a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-25
- Deleting a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-25
- Changing a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-26

- Adding a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-26
- Deleting a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-26
- Changing a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only), page 32-27

# Viewing the Cisco Unity Connection Root Certificate

The root certificate is used by SCCP integrations with Cisco Unified Communications Manager 4.1 and later and SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports. You can view the root certificate to help troubleshoot authentication and encryption problems.

### To View the Cisco Unity Connection Root Certificate

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **Root Certificate**.

**Step 2** On the **View Root Certificate** page, the information from the root certificate is displayed.

# Saving the Cisco Unity Connection Root Certificate as a File

The root certificate is used by SCCP integrations with Cisco Unified CM 4.1 and later and SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

### To Save the Cisco Unity Connection Root Certificate as a File

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **Root Certificate**.

**Step 2** On the **View Root Certificate** page, right-click the **Right-Click to Save the Certificate as a File** link, and select **Save Target As**.

**Step 3** In the **Save As** dialog box, browse to the location where you want to save the Unity Connection root certificate as a file.

**Step 4** In the File Name field, confirm that the filename has the correct extension, depending on the version of Cisco Unified CM:

- For Cisco Unified CM 5.x or later, confirm that the extension is .pem (rather than .htm).
- For Cisco Unified CM 4.x, confirm that the extension is .0 (rather than .htm).

**Caution** The certificate must be saved as a file with the correct extension or Cisco Unified CM will not recognize the certificate.

**Step 5** Select **Save**.

**Step 6** In the **Download Complete** dialog box, select **Close**.

**Step 7** The Unity Connection root certificate file is ready to be copied to all Cisco Unified CM servers in this Cisco Unified CM phone system integration. For instructions, see the applicable Cisco Unified CM integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

# Adding a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

The SIP certificate is used only by SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

### To Add a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificate**.

**Step 2** On the **Search SIP Certificates** page, select **Add New**.

**Step 3** On the **New SIP Certificate** page, in the **Display Name** field, enter a display name for the SIP certificate.

**Step 4** In the **Subject Name** field, enter a subject name that matches the X.509 subject name of the SIP security profile for the SIP trunk in Cisco Unified CM Administration.

**Caution** This subject name must match the X.509 subject name of the SIP security profile used by Cisco Unified CM. Otherwise, Cisco Unified CM authentication and encryption fail.

**Step 5** Select **Save**.

# Deleting a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can delete a SIP certificate when the Cisco Unified CM server is no longer configured for authentication of the Cisco Unity Connection voice messaging ports.

### To Delete a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificate**.

**Step 2** On the **Search SIP Certificates** page, check the check box next to the display name of the SIP certificate that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the SIP certificate, select **OK**.

# Changing a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can change a SIP certificate after it is created.

### To Change a SIP Certificate (Cisco Unified Communications Manager SIP Trunk Integrations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Certificate**.

**Step 2** On the **Search SIP Certificates** page, select the name of the SIP certificate that you want to change.

**Step 3** On the **Edit SIP Certificate** page, enter the applicable settings and select **Save**.

# Adding a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

The SIP security profile is used only by SIP trunk integrations with Cisco Unified CM 7.0 and later, and is required for authentication of the Cisco Unity Connection voice messaging ports.

### To Add a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

**Step 2** On the **Search SIP Security Profiles** page, select **Add New**.

**Step 3** On the **New SIP Security Profile** page, in the **Port** field, enter the port number that the Cisco Unified CM server uses for SIP trunk authentication and encryption of the voice messaging ports.

**Step 4** To encrypt the call signaling messages, check the **Do TLS** check box.

**Step 5** Select **Save**.

# Deleting a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can delete a SIP security profile when the Cisco Unified CM server is no longer configured for authentication of the Cisco Unity Connection voice messaging ports.

**To Delete a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)**

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

**Step 2** On the **Search SIP Security Profiles** page, check the check box next to the display name of the SIP security profile that you want to delete.

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

**Step 4** When prompted to confirm that you want to delete the SIP security profile, select **OK**.

## Changing a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)

You can change a SIP security profile after it is created.

**To Change a SIP Security Profile (Cisco Unified Communications Manager SIP Trunk Integrations Only)**

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations > Security**, then select **SIP Security Profile**.

**Step 2** On the **Search SIP Certificates** page, select the name of the SIP security profile that you want to change.

**Step 3** On the **Edit SIP Security Profile** page, enter the applicable settings and select **Save**.

# IPv6 in Cisco Unity Connection (Cisco Unified Communications Manager Integrations Only)

Cisco Unity Connection supports IPv6 addressing with Cisco Unified Communications Manager phone system integrations using SCCP or SIP.

IPv6 support is disabled by default. When you enable IPv6, you can configure Unity Connection to obtain an IPv6 address either through router advertisement, through DHCP, or by manually configuring an address. You can also configure the mode in which Unity Connection listens for incoming traffic—IPv4, IPv6, or both IPv4 and IPv6.

For SCCP integrations with Cisco Unified CM, if Unity Connection is configured to listen for incoming IPv4 and IPv6 traffic, you can configure the addressing mode that Unity Connection uses for call control signaling for each port group to use either IPv4 or IPv6. (This mode is also used when connecting to a TFTP server.)

For SIP integrations with Cisco Unified CM, if Unity Connection is configured to listen for incoming IPv4 and IPv6 traffic, you can configure the addressing mode that Unity Connection uses for call control signaling for each port group to use either IPv4 or IPv6. (This mode is also used when connecting to a TFTP server.) In addition, you can configure the addressing mode that Unity Connection uses for media for each port group to use either IPv4 or IPv6.

Note the following considerations when deploying IPv6 for Cisco Unified CM integrations:

- IPv6 is supported in Cisco Unified CM release 7.1(2) and later.
- The CTL file required for security features (authentication and encryption) for SCCP integrations uses IPv4 addressing. Therefore, in order to use authentication and encryption with SCCP secure ports, you must retain the IPv4 address or host name for the Cisco Unified CM server(s) on the port group in Unity Connection.
- Some versions of Cisco Adaptive Security Appliance (ASA) do not support application inspection for IPv6 traffic for Unified Communications application servers and endpoints. We recommend not using IPv6 for Unified Communications if you are using a Cisco ASA version that does not provide this support. See the documentation for your version of Cisco ASA to determine whether application inspection is supported in your deployment.

For instructions on enabling and configuring IPv6 for an existing Cisco Unified CM integration, see the "Adding or Changing the IPv6 Addresses of Cisco Unity Connection Servers" chapter of the *Upgrade Guide for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html. For instructions on enabling and configuring IPv6 while setting up a new Cisco Unified CM integration, see the applicable Cisco Unified CM integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

# Creating a Cisco Unified Mobility Advantage Integration in Cisco Unity Connection 10.x

See the following sections:


- About the Cisco Unified Mobility Advantage Integration in Cisco Unity Connection 10.x, page 33-1
- Task List for Creating an Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage, page 33-1
- Configuring Cisco Unity Connection 10.x for a Cisco Unified Mobility Advantage Integration, page 33-2
- Testing the Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage, page 33-3


## About the Cisco Unified Mobility Advantage Integration in Cisco Unity Connection 10.x

The Cisco Unified Mobility Advantage integration provides Cisco Unified Mobile Communicator users with access to their Cisco Unity Connection voice messages through Cisco Unified Mobile Communicator on their phones. This allows users to do the following:

- Hear an alert when new voice messages arrive.
- View a list of voice messages.
- Listen to voice messages.
- Delete voice messages.

## Task List for Creating an Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage

1. Review the system requirements to confirm that all requirements for Cisco Unified Mobility Advantage and the Cisco Unity Connection server have been met. See the "Requirements" section on page 33-2.

2. Configure Cisco Unified Mobility Advantage. See the "Configuring Cisco Unified Mobility Advantage" chapter of the *Installation and Upgrade Guide for Cisco Unified Mobility Advantage, Release 7.0* at http://cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.
3. Provision Cisco Unified Mobility Advantage. See the *Cisco Unified Mobility Advantage 7.0 Provisioning Guide* at http://cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.

**Note** Cisco Unified Mobility Advantage must have an end user for each Cisco Unity Connection user that accesses Cisco Unity Connection voice messages through Cisco Unified Mobile Communicator.

4. Configure Cisco Unity Connection. See the "Configuring Cisco Unity Connection 10.x for a Cisco Unified Mobility Advantage Integration" section on page 33-2.
5. Test the integration with Cisco Unified Mobility Advantage. See the "Testing the Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage" section on page 33-3.

## Requirements

The integration with Cisco Unified Mobility Advantage has the following requirements:

- Cisco Unified Mobility Advantage 7.0 or later is installed according to the "Installing Cisco Unified Mobility Advantage" chapter of the *Installation and Upgrade Guide for Cisco Unified Mobility Advantage, Release 7.0* at http://cisco.com/en/US/products/ps7270/prod_installation_guides_list.html.
- Cisco Unity Connection is installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring Cisco Unity Connection 10.x for a Cisco Unified Mobility Advantage Integration

Do the following procedure.

**To Configure Cisco Unity Connection for a Cisco Unified Mobility Advantage Integration**

**Step 1** Sign in to Cisco Unity Connection Administration as a user that is assigned to the Remote Administration role.

**Step 2** Expand **Class of Service**, then select **Class of Service**.

**Step 3** On the **Search Class of Service** page, select the class of service for the Cisco Unified Mobile Communicator end users who will have access to voice messages in Unity Connection.

**Step 4** On the **Edit Class of Service** page, under **Licensed Features**, check the **Allow Users to Access Voicemail Using an IMAP Client and/or Single Inbox** check box and select one of the following options:

- Allow IMAP Users to Access Message Bodies
- Allow IMAP Users to Access Message Bodies Except on Private Messages

- Allow IMAP Users to Access Message Headers Only

On the **Edit Class of Service** page, under **Licensed Features,** check the **Allow Users to Access Voicemail Using an IMAP Client** check box and select one of the following options:

- Allow Users to Access Message Bodies
- Allow Users to Access Message Bodies Except on Private Messages
- Allow Users to Access Message Headers Only

**Step 5** Select **Save**.

**Step 6** Repeat Step 3 through Step 5 for all remaining classes of service for the Cisco Unified Mobile Communicator end users who will have access to voice messages in Unity Connection.

# Testing the Integration of Cisco Unity Connection 10.x with Cisco Unified Mobility Advantage

Do the following procedure.

### To Test the Configuration

**Step 1** From a phone, leave a message at the Cisco Unity Connection extension for a Cisco Unified Mobile Communicator user.

**Step 2** By using Cisco Unified Mobile Communicator on the phone of the Cisco Unified Mobile Communicator user, confirm that the new voice message appears in the list of voice messages.

**Step 3** Confirm that you can listen to the new voice message in Cisco Unified Mobile Communicator.

**Step 4** Delete the new voice message in Cisco Unified Mobile Communicator.

# Creating a Cisco Fax Server Integration in Cisco Unity Connection 10.x

See the following sections:


- About the Cisco Fax Server Integration in Cisco Unity Connection 10.x, page 34-1
- Task List for Creating a Cisco Fax Server Integration in Cisco Unity Connection 10.x, page 34-2
- Configuring the Cisco Fax Server in Cisco Unity Connection 10.x, page 34-3
- Configuring Cisco Unity Connection 10.x for the Cisco Fax Server Integration, page 34-6
- Configuring Cisco Unity Connection 10.x Users for the Cisco Fax Server Integration, page 34-7
- Testing the Cisco Fax Server Integration in Cisco Unity Connection 10.x, page 34-7
- Changing the Cisco Unity Connection 10.x Configuration for the Cisco Fax Server Integration, page 34-8
- Changing the Cisco Unity Connection 10.x User Configuration for the Cisco Fax Server Integration, page 34-9
- Configuring a Single Number to Receive Both Voice Calls and Faxes in Cisco Unity Connection 10.x, page 34-9


## About the Cisco Fax Server Integration in Cisco Unity Connection 10.x

Cisco Unity Connection can integrate with the Cisco Fax Server so that users can do the following while on the phone or while using the Unity Connection Web Inbox or Messaging Inbox:

- Receive faxes that are sent to the fax extension for the user. Depending on the system configuration, faxes will be available in the user mailboxes or in the user IMAP clients.
- Forward the faxes that they receive to a fax machine for printing.
- Forward the faxes that they receive to another user.

Inbound faxes are sent to the fax extension for the user. The Cisco Fax Server uses its email gateway to route the fax through SMTP to the user mailbox on the Unity Connection server. The Text to Speech (TTS) feature cannot read faxes.

**Note** You must manage and configure the Cisco Fax Server on the Cisco Fax Server, not in Cisco Unity Connection Administration.

The Cisco Fax Server handles the following functions:

- Routing inbound faxes to user mailboxes.
- Managing inbound and outbound faxes.
- Writing logs for inbound and outbound faxes.
- Generating reports for monitoring Cisco Fax Server statistics.
- Sending alerts to the administrator.
- Providing cover pages.
- Providing least-cost routing.

# Task List for Creating a Cisco Fax Server Integration in Cisco Unity Connection 10.x

1. Review the system requirements to confirm that all requirements for the Cisco Fax Server and the Cisco Unity Connection server have been met. See the "Requirements" section on page 34-2.
2. Configure the Cisco Fax Server. See the "Configuring the Cisco Fax Server in Cisco Unity Connection 10.x" section on page 34-3.
3. Configure Cisco Unity Connection. See the "Configuring Cisco Unity Connection 10.x for the Cisco Fax Server Integration" section on page 34-6.
4. Configure the Unity Connection user accounts. See the "Configuring Cisco Unity Connection 10.x Users for the Cisco Fax Server Integration" section on page 34-7.
5. Test the Cisco Fax Server integration. See the "Testing the Cisco Fax Server Integration in Cisco Unity Connection 10.x" section on page 34-7.

**Note** You can change the Cisco Unity Connection configuration and the user configuration after the Cisco Fax Server integration is created. See the "Changing the Cisco Unity Connection 10.x Configuration for the Cisco Fax Server Integration" section on page 34-8 and the "Changing the Cisco Unity Connection 10.x User Configuration for the Cisco Fax Server Integration" section on page 34-9.

## Requirements

The Cisco Fax Server integration has the following requirements:

- Cisco Fax Server 9.0 or later installed as described in the *Cisco Fax Server Installation Guide* at http://www.cisco.com/en/US/products/ps6178/prod_installation_guides_list.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring the Cisco Fax Server in Cisco Unity Connection 10.x

Do the following four procedures in the order given.

**Note** The Cisco Fax Server documentation is available at http://www.cisco.com/en/US/products/ps6178/tsd_products_support_series_home.html.

### To Configure SMTP on the Cisco Fax Server

**Step 1** To sign in to the Cisco Fax Server, on the Start menu, select **All Programs > RightFax Enterprise Fax Manager**.

**Step 2** In the left pane of the **RightFax Enterprise Fax Manager** window, select the name of the Cisco Fax Server.

**Step 3** In the right pane, under **Service Name**, scroll down to RightFax eTransport Module.

**Step 4** Right-click **RightFax eTransport Module** and select **Configure Services**.

**Step 5** Select the **eTransport** tab.

**Step 6** In the **SMTP Hostname** field, enter the IP address of the Unity Connection server.

**Step 7** Select the **Custom Messages** tab.

**Step 8** In the applicable fields, enter **[Fax Failure]** for the fax failure prefix before the beginning word of the text. The following fields are recommended for entering the fax failure prefix:

- Imaging Error
- Bad Form Type
- Bad Fax Phone Number
- Too Many Retries
- Sending Error
- Incomplete Fax
- Invalid Billing Code
- Fax Needs Approval
- Fax Number Blocked
- Human Answered Fax
- Fax Block by Do Not Dial

When the text at the beginning of the field matches the value for the **Subject Prefix for Notification of a** Failed Fax field on the **System Settings > Advanced > Fax** page of Cisco Unity Connection Administration, Unity Connection notifies the user of the failed fax.

**Step 9** In the **Successful Send** field, enter **[Fax Success]** for the fax success prefix before the beginning word of the text.

When the text at the beginning of the field matches the value for the **Subject Prefix for Notification of a Successful Fax** field on the **System Settings > Advanced > Fax** page of Connection Administration, Unity Connection notifies the user of the successful fax.

**Step 10** Select **OK**.

### To Set Up the Windows Email Service for POP3

**Step 1** On the Cisco Fax Server, on the Windows Start menu, select **Control Panel > Add or Remove Programs**.

**Step 2** In the **Add or Remove Programs** window, in the left pane, select **Add/Remove Windows Components**.

**Step 3** In the **Windows Components** wizard, on the **Windows Components** page, check the **E-mail Services** check box and select **Next**.

**Step 4** On the Completing the **Windows components Wizard** page, select **Finish**.

**Step 5** Close the **Add or Remove Programs** window.

**Step 6** On the **Windows Start** menu, select **All Programs > Administrative Tools > POP3 Service**.

**Step 7** In the POP3 Service window, in the left pane, expand the Cisco Fax Server and select the Cisco Fax Server node.

**Step 8** In the right pane, select **Add Mailbox**.

**Caution** A domain for the POP3mailbox must be configured on the Cisco Fax Server. Otherwise, this option will not be available.

**Step 9** In the **Add Mailbox** dialog box, in the **Mailbox Name** field, enter a name for the mailbox that receives faxes on the Cisco Fax Server.

**Step 10** In the **Password** field, enter a password for this mailbox.

**Note** Make a note of this password because you will enter it in the "To Configure the POP3 Mailbox on the Cisco Fax Server" procedure on page 34-4.

**Step 11** In the **Confirm Password** field, re-enter the password and select **OK**.

### To Configure the POP3 Mailbox on the Cisco Fax Server

**Step 1** In the **RightFax Enterprise Fax Manager** window, in the right pane, under **Service Name**, scroll down to **RightFax E-mail Gateway Module**.

**Step 2** Right-click **RightFax E-mail Gateway Module** and select **Configure Service**.

**Step 3** In the **E-mail configuration** dialog box, select **Add Gateway**.

**Step 4** In the **E-mail Gateway Selection** dialog box, select **SMTP/POP3** and select **Select**.

**Step 5** On the **General** tab, in the **Server Address** field, enter the IP address of the Cisco Fax Server.

**Step 6** In the **POP3 Mailbox Name** field, enter **<POP3 mailbox name>@<Cisco Fax Server name>**.

**Step 7** In the **Mailbox Password** field, enter the password for the POP3 mailbox that you entered in the "To Set Up the Windows Email Service for POP3" procedure on page 34-4.

**Step 8** Uncheck the **Use IETF Fax Addressing** check box.

**Step 9** Confirm that the **Send Through Default User When E-mail Sender Is Unknown** check box is checked.

**Step 10** In the **Email Delivery Direction** field, confirm that **Both** is selected.

**Step 11** Select **OK**.

### To Configure IIS Relay for the POP3 Mailbox on the Cisco Fax Server

**Step 1** On the Windows Start menu, select **Programs > Administrative Tool > Internet Information Services (IIS) Manger**.

**Step 2** In the Internet Information Services (IIS) Manager window, in the left pane, under the RightFax node, right-click **Default SMTP Virtual Server** and select **Properties**.

**Step 3** In the **Default SMTP Virtual Server Properties** dialog box, select the **Access** tab.

**Step 4** Under **Relay Restrictions**, select **Relay**.

**Step 5** In the **Relay Restrictions** dialog box, confirm that **Only the List Below** is selected.

**Step 6** Under **Computers**, select **Add**.

**Step 7** In the **Computer** dialog box, select **Single Computer** and enter the IP address of the Cisco Fax Server.

**Step 8** Select **OK**.

**Step 9** In the **Relay Restrictions** dialog box, select **OK**.

**Step 10** In the **Default SMTP Virtual Server Properties** dialog box, select **OK**.

**Step 11** Close the **Internet Information Services (IIS) Manager** window.

### To Add Unity Connection Users to the Cisco Fax Server

**Step 1** In the **RightFax Enterprise Fax Manager** window, in the right pane, right-click **Users** and select **New**.

**Step 2** In the **User Edit** dialog box, in the **User ID** field, enter the alias for the Unity Connection user.

**Step 3** In the **User Name** field, enter the name of the Unity Connection user.

**Step 4** In the **Group ID** field, confirm that **Everyone** is selected.

**Step 5** In the **Voicemail Subscriber ID** field, enter the extension for the Unity Connection user.

**Step 6** In the **E-mail Address** field, enter **<Unity Connection user alias>@<fully qualified DNS name of the Unity Connection server>**.

**Step 7** Select the **Inbound Routing** tab.

**Step 8** In the **Routing Code (DID/DNIS Number)** field, enter the extension of the Unity Connection user.

**Step 9** In the **Routing Type** field, select **SMTP**.

**Step 10** Select the **Notification** tab.

**Step 11** In the **Method** field, select **SMTP**.

**Step 12** In the **Notification Address/Info** field, enter **<Unity Connection user alias>@<Unity Connection server name>**.

**Step 13** Select **OK**.

**Step 14** Repeat Step 1 through Step 13 for all remaining users who will receive faxes.

**Step 15** Close the **RightFax Enterprise Fax Manager** window.

# Configuring Cisco Unity Connection 10.x for the Cisco Fax Server Integration

Do the following procedures.

### To Allow Cisco Unity Connection to Access the IP Address Access of the Cisco Fax Server

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **SMTP Configuration > Server**.

**Step 2** On the **SMTP Server Configuration** page, in the **Edit** menu, select **Search IP Address Access List**.

**Step 3** On the **Search IP Address Access List** page, select **Add New**.

**Step 4** On the **New Access IP Address** page, in the **IP Address** field, enter the IP address of the Cisco Fax Server.

**Step 5** Select **Save**.

**Step 6** Check the **Allow Unity Connection** check box and select **Save**.

### To Enable the Cisco Fax Server Integration on Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Fax Server**.

**Step 2** On the **Edit Fax Server** page, check the **Enabled** check box.

**Step 3** In the **Fax Server Name** field, enter a descriptive name for the Cisco Fax Server.

**Step 4** In the **SMTP Address** field, enter the fully qualified SMTP address of the SMTP server on the Cisco Fax Server.

**Caution** This fully qualified SMTP address must match the server address and domain that are configured for the POP3 mailbox on the Cisco Fax Server. Otherwise, the integration will not function correctly.

**Step 5** In the **IP Address** field, enter the IP address of the Cisco Fax Server.

**Step 6** If you use a smart host SMTP server to deliver faxes from the Cisco Fax Server to Cisco Unity Connection, check the **Use Smart SMTP Host** check box. Otherwise, uncheck this check box.

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

### To Customize the Cisco Fax Server Integration on Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Fax**.

**Step 2** In the **Fax Configuration** page, in the **Faxable File Types** field, enter the file extensions (separated by a comma) that Unity Connection keeps in messages that are delivered to the Cisco Fax Server. Unity Connection removes all files with other file extensions before delivering the message to the Cisco Fax Server.

**Step 3** In the **Subject Prefix for Notification of a Successful Fax** field, enter the prefix that the Cisco Fax Server adds to the Subject field of fax reports. When Unity Connection detects this prefix, it generates a delivery receipt and places it in the user mailbox.

**Step 4** In the **Subject Prefix for Notification of a Failed Fax** field, enter the prefix that the Cisco Fax Server adds to the Subject field of fax reports. When Unity Connection detects this prefix, it generates a non-delivery receipt and places it in the user mailbox.

**Step 5** Select **Save**.

# Configuring Cisco Unity Connection 10.x Users for the Cisco Fax Server Integration

Do the following procedure.

**Note** The Cisco Fax Server must have a subscriber for each Unity Connection user that you are configuring.

While on the phone, users can add or change the number for the fax machine that they send faxes to for printing.

### To Configure Users

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Note** If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

**Step 3** On the **Edit User Basics** page, in the **Outgoing Fax Number** field, enter the number for the fax machine that users send faxes to for printing.

**Step 4** In the **Outgoing Fax Server** field, select the name of the Cisco Fax Server.

**Step 5** Select **Save**.

**Step 6** Repeat Step 2 through Step 5 for all remaining users.

**Note** You can use **Bulk Edit** mode to add or change fax extensions for multiple users at once.

# Testing the Cisco Fax Server Integration in Cisco Unity Connection 10.x

Do the following procedure.

### To Test the Cisco Fax Server Integration

**Step 1** Send a fax to the fax extension of a user who has been configured for the Cisco Fax Server integration.

**Step 2** Sign in to the Cisco Unity Connection mailbox of the user to whom you sent the fax.

**Step 3** If the user account is configured for speech access, say **Play Messages**.

If the user account is not configured for speech access, press **1**, and then follow the prompts to list messages.

**Step 4** When you hear the system announce the fax that you just sent, either say **Fax**, or press the applicable keys on the phone keypad to print the fax.

# Changing the Cisco Unity Connection 10.x Configuration for the Cisco Fax Server Integration

You can change the Cisco Unity Connection configuration after the Cisco Fax Server integration was created. Do the applicable procedures.

### To Change the Cisco Fax Server Integration on Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Fax Server**.

**Step 2** On the **Edit Fax Server Configuration** page, check the **Enabled** check box to enable the integration with the Cisco Fax Server. Otherwise, uncheck this check box.

**Step 3** In the **Fax Server Name,** enter a descriptive name for the Cisco Fax Server.

**Step 4** In the **SMTP Address** field, enter the fully qualified SMTP address of the SMTP server on the Cisco Fax Server.

**Step 5** In the **IP Address** field, enter the IP address of the Cisco Fax Server.

**Step 6** If you use a smart host SMTP server to deliver faxes from the Cisco Fax Server to Cisco Unity Connection, check the **Use Smart SMTP Host** check box. Otherwise, uncheck this check box.

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

### To Change the Customized Settings for the Cisco Fax Server Integration on Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Advanced > Fax**.

**Step 2** In the **Fax Configuration** page, in the **Faxable File Types** field, enter the file extensions (separated by a comma) that Unity Connection keeps in messages that are delivered to the Cisco Fax Server. Unity Connection removes all files with other file extensions before delivering the message to the Cisco Fax Server.

**Step 3** In the **Subject Prefix for Notification of a Successful Fax** field, enter the prefix that the Cisco Fax Server adds to the Subject field of fax reports. When Unity Connection detects this prefix, it generates a delivery receipt and places it in the user mailbox.

**Step 4** In the **Subject Prefix for Notification of a Failed Fax** field, enter the prefix that the Cisco Fax Server adds to the Subject field of fax reports. When Unity Connection detects this prefix, it generates a non-delivery receipt and places it in the user mailbox.

**Step 5** Select **Save**.

# Changing the Cisco Unity Connection 10.x User Configuration for the Cisco Fax Server Integration

You can change the user configuration after the Cisco Fax Server integration was created. Do the following procedure.

**Note** While on the phone, users can add or change the number for the fax machine that they send faxes to for printing.

### To Change the User Configuration for the Cisco Fax Server Integration

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Note** If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

**Step 3** On the **Edit User Basics** page, in the **Outgoing Fax Number** field, enter the number for the fax machine that users send faxes to for printing.

**Step 4** In the **Outgoing Fax Server** field, select the name of the Cisco Fax Server.

**Step 5** Select **Save**.

**Step 6** Repeat Step 2 through Step 5 for all remaining users.

**Note** You can use **Bulk Edit** mode to change fax extensions for multiple users at once.

# Configuring a Single Number to Receive Both Voice Calls and Faxes in Cisco Unity Connection 10.x

Cisco Unity Connection can use a single number to receive both voice calls and fax calls. In this configuration, incoming calls are directed to a Cisco gateway that can detect a CNG (fax) tone. When a CNG tone is detected, the gateway forwards the fax call to the Cisco Fax Server. When no CNG tone is detected, the gateway forwards the voice call to Unity Connection.

# Task List

1. Download the TCL script file app_fax_detect.2.1.2.3.tcl or later. See the "Configuring Fax Detection" chapter of the applicable *Cisco IOS Fax and Modem Services over IP Application Guide* at http://www.cisco.com/cisco/web/psa/default.html?mode=prod.
2. Configure the Cisco IOS gateway for fax detection. See the "Configuring T.38 Fax Relay" chapter of the applicable *Cisco IOS Fax and Modem Services over IP Application Guide* at http://www.cisco.com/cisco/web/psa/default.html?mode=prod.

# Requirements

- Cisco Fax Server 9.0 or later installed as described in the *Cisco Fax Server Installation Guide* at http://www.cisco.com/en/US/products/ps6178/prod_installation_guides_list.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.
- The TCL script file app_fax_detect.2.1.2.3.tcl or later.

# Managing SpeechView Transcription Error Codes in Cisco Unity Connection

See the following sections:


- Overview of SpeechView Transcription in Cisco Unity Connection, page 35-1
- Default Transcription Error Codes in Cisco Unity Connection, page 35-2
- Add New Transcription Error Code in Cisco Unity Connection, page 35-2
- Modifying the Transcription Error Code in Cisco Unity Connection, page 35-3
- Deleting the Transcription Error Code in Cisco Unity Connection, page 35-4
- Search the Transcription Error Codes in Cisco Unity Connection, page 35-4


## Overview of SpeechView Transcription in Cisco Unity Connection

When a sender sends a voice mail to a SpeechView user, the received voice message is sent to the third-party external transcription service. The transcription of voice messages is sent back to Cisco Unity Connection. However, in case of any transcription failure, the third-party external transcription service sends an error code to Unity Connection.

Cisco Unity Connection Administration interface shows the five default error codes that can be sent by the third-party external transcription service. Only the administrator has the privileges to modify/delete the existing error code and the associated description. In addition, he or she has the privilege to add a new error code. Whenever a new error code is sent by the third-party external transcription service, the administrator needs to add a new error code along with the appropriate description.

Note the following:

- The error code and the error code description should be in the default system language.
- If the error code provisioning is not done, then the error code received from the third-party external transcription service will be displayed.

**Note** In Cisco Unity Connection, to avoid timeout or failure of the registration request with the third-party external transcription service, make sure to:

- Remove the email disclaimers from the inbound and the outbound email messages between Unity Connection and the third-party external transcription service.

- Maintain the SpeechView registration messages in the S/MIME format.

# Default Transcription Error Codes in Cisco Unity Connection

In Cisco Unity Connection Administration page> Unified Messaging> SpeechView Transcription, when you select **Error Codes**, then on the Search Transcription Error Codes page, the default error codes appear on the screen. These default error codes are sent by the third-party external transcription service to the SpeechView user. The Table 35-1 shows the default error codes in the Cisco Unity Connection Administration interface.

*Table 35-1 Default Error Codes*

| Error Code Name | Description |
|---|---|
| Fault | Registration Failed<br>When Unity Connection tries to register with the third-party external transcription service and the registration fails. |
| Inaudible | The system was unable to transcribe the message<br>When a voice mail sent by a SpeechView user is inaudible at the third-party external transcription service site. |
| Rejected | The system was unable to transcribe the message<br>When the third-party external transcription service is not able to transcript the voice mail sent by a SpeechView user. |
| Time-out | The transcription request timed out<br>Whenever there is a response timeout from the third-party external transcription service. |
| Unconverted | The transcription has failed. Call voice mail to hear the message<br>When the conversion request contains more than one audio file attachment, the third-party external transcription service rejects the messages. |

**Note** The bold text in the table above shows the default error code description displayed to the user.

# Add New Transcription Error Code in Cisco Unity Connection

**To add a New Transcription Error Code**

**Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging> SpeechView Transcription**, then select **Error Codes**.

**Step 2** On the **Search Transcription Error Codes** page, select **Add New**.

**Step 3** On the **New Transcription Error Code** page, enter the error code and the error code description to create a new error code.

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** To save and search the existing server codes on the **New Transcription Error Code** page, select the **Transcription Error Code** menu.

**Step 6** To clear-off the new error code values before saving, select the **Reset** menu.

See Also

- New Transcription Error Code, page 9-31

# Modifying the Transcription Error Code in Cisco Unity Connection

### To Modify a Transcription Error Code

**Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging> SpeechView Transcription**, then select **Error Codes**.

**Step 2** On the **Search Transcription Error Codes** page, select the display name of the error code that you want to modify.

**Note** If the error code that you want to modify does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 3** On the **Edit Transcription Error Code (Fault)** page, change the error code or the error code description, as applicable.

**Step 4** When you have finished changing settings on the **Edit Transcription Error Code (Fault)** page, select **Save**.

See Also

- Edit Transcription Error Code, page 9-31

# Deleting the Transcription Error Code in Cisco Unity Connection

### To Delete a Transcription Error Code

**Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging> SpeechView Transcriptions**, then select **Error Codes**.

**Step 2** On the **Search Transcription Error Code** page, check the check box adjacent to the display name of the schedule that you want to delete.

**Note** If the error code that you want to delete does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

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

**Step 4** In the dialog box that asks you to confirm the deletion, select **OK**.

See Also

- Delete Transcription Error Code, page 9-32

# Search the Transcription Error Codes in Cisco Unity Connection

### To a search Transcription Error Code

**Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging> SpeechView Transcription**, then select **Error Codes**.

**Step 2** On the **Search Transcription Error Codes** page, select **Error Codes** or **Error Code Desc** from the drop-down list.

**Step 3** Enter the error code or error code description in the text box.

**Step 4** Select **Find**.

See Also

- Search Transcription Error Codes, page 9-30

# Creating Calendar and Contact Integrations in Cisco Unity Connection

See the following sections:


- About Calendar Integrations in Cisco Unity Connection, page 36-1
- About Contact Integrations in Cisco Unity Connection, page 36-2
- Creating a Calendar and Contact Integration with Exchange 2007 in Cisco Unity Connection, page 36-2
- Creating a Calendar and Contact Integration with Exchange 2003 in Cisco Unity Connection, page 36-9
- Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace in Cisco Unity Connection, page 36-16
- Creating a Calendar Integration with Cisco Unified MeetingPlace Express in Cisco Unity Connection, page 36-21


For information on configuring calendar and contact integrations in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Microsoft Exchange for Unified Messaging" chapter and/or the "Configuring Cisco Unity Connection 10.x and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

# About Calendar Integrations in Cisco Unity Connection

When integrated with supported calendar applications (Exchange 2007, Exchange 2003, Cisco Unified MeetingPlace, or Cisco Unified MeetingPlace Express), Cisco Unity Connection enables users to do the following by phone:

- Hear a list of upcoming meetings (Outlook meetings only).
- Join a meeting that is in progress (MeetingPlace and MeetingPlace Express meetings only).
- Hear a list of the participants for a meeting.
- Send a message to the meeting organizer.
- Send a message to the meeting participants.
- Accept or decline meeting invitations (Outlook meetings only).
- Set up immediate meetings (MeetingPlace and MeetingPlace Express meetings only).

- Cancel a meeting (meeting organizers only).

# About Contact Integrations in Cisco Unity Connection

When integrated with Exchange 2007 or Exchange 2003, Cisco Unity Connection enables users to import Exchange contacts by using the Unity Connection Messaging Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Connection Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

# Creating a Calendar and Contact Integration with Exchange 2007 in Cisco Unity Connection

If you have Exchange 2007 installed, you can integrate Cisco Unity Connection with Exchange 2007 so that users can do the following:

- Review upcoming meetings by phone.
- Import Exchange contacts. The contact information can be used in rules that users create in the Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

For information on configuring calendar and contact integrations in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Microsoft Exchange for Unified Messaging " chapter and/or the "Configuring Cisco Unity Connection 10.x and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

## Task List for Creating a Calendar and Contact Integration with Exchange 2007 in Cisco Unity Connection

1. Review the system requirements to confirm that all requirements for Exchange 2007 and the Cisco Unity Connection server have been met. See the "Requirements for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection" section on page 36-3.
2. Configure Exchange 2007. See the "Configuring Exchange 2007 for the Calendar and Contact Integration in Cisco Unity Connection" section on page 36-3.
3. Configure Unity Connection. See the "Configuring Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration" section on page 36-6.
4. *(When enabling personal call transfer rules only)* Verify that the users or templates are assigned to a class of service that enables them to use the personal call transfer rules feature.
5. Configure the Unity Connection users. See the "Configuring Users for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection" section on page 36-7.
6. Test the calendar integration. See the "Testing the Exchange 2007 Calendar Integration in Cisco Unity Connection" section on page 36-8.
7. To teach users how to use the Unity Connection calendar, refer them to the following:

- For listing, joining, and scheduling meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/phone/b_10xcucugphone.html.
- For importing Exchange contacts, see the "Managing Your Personal Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html.
- For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/pctr/b_10xcucugpctr.html.

# Requirements for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection

The calendar and contact integration with Exchange 2007 has the following requirements:

- Exchange 2007 as described in the "Requirements for Accessing Calendar Information for Meetings" and "Requirements for Accessing Exchange Contact Information" sections of *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring Exchange 2007 for the Calendar and Contact Integration in Cisco Unity Connection

Do the following tasks to configure Exchange 2007 for the calendar and contact integration:

1. Confirm that the Exchange 2007 server has been configured to include the "Client Access" role.
2. Do the "To Configure Access to Exchange 2007 for the Calendar and Contact Integration in Cisco Unity Connection" procedure on page 36-3.
3. *(Optional)* If you are using SSL for secure access to the Exchange 2007 server, do the "To Configure Secure Access to Exchange 2007 for the Calendar and Contact Integration (With SSL) in Cisco Unity Connection" procedure on page 36-4.

### To Configure Access to Exchange 2007 for the Calendar and Contact Integration in Cisco Unity Connection

**Step 1** On the Exchange server, open the **Internet Services (IIS) Manager** application.

**Step 2** Go to **Internet Information Services > <server name> > Web Sites > Default Web Site**.

**Step 3** Right-click **Exchange** and select **Properties**.

**Step 4** In the **Exchange Properties** dialog box, select the **Virtual Directory** tab.

**Step 5** Under Content For This Resource Should Come From, select **A Directory Located On This Computer.**

**Step 6** Confirm the Local Path is set to **\\.\BackOfficeStorage\<your-domain.com>\MBX**.

**Step 7** Select the **Read** check box.

**Step 8** Select the **Directory Security** tab.

**Step 9** Under **Authentication and Access Control,** select **Edit**.

**Step 10** In the **Authenticated Access section of the Authentication Methods** dialog box, check the check boxes for one or more of the following options:

- Integrated Windows authentication (sometimes referred to as NTLM)
- Basic Authentication
- Digest Authentication for Windows Domain Servers

**Step 11** Select **OK**.

**Step 12** In the **Exchange Properties** dialog box, select **OK**.

**Step 13** Go to **Internet Information Services > <server name> > Web Service Extensions**.

**Step 14** In the right-hand pane, select **WebDav** and confirm that the status is "Allowed." If the status is not "Allowed", click **Allow.**

**Step 15** On the Exchange server, open the **Exchange Management Console**.

**Step 16** Go to **Server Configuration > Mailbox.**

**Step 17** Do the following for each mailbox that you want to configure for the calendar and contact integration:

**a.** In the upper middle pane, select the mailbox name.

**b.** In the lower middle pane, select the **WebDav** tab.

**c.** Right-click **Exchange (Default Web Site)** and select **Properties**.

**d.** In the **Exchange (Default Web Site) Properties** dialog box, select the **Authentication** tab.

**e.** Select **Use One or More Standard Authentication Methods** and select the same authentication method(s) that you configured in Step 10.

**Step 18** Click **OK**.

**Step 19** Open the **Exchange Management Shell**.

**Step 20** In the **Exchange Management Shell**, enter the following command:

**iisbreset /noforce**

**Step 21** Press **Enter**.

### To Configure Secure Access to Exchange 2007 for the Calendar and Contact Integration (With SSL) in Cisco Unity Connection

**Note** If you have already configured secure IMAP with SSL and have enabled the certificate for both IMAP and IIS, then you can skip the following procedure and continue with the "Configuring Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration" section on page 36-6.

**Step 1** On the Exchange Server, open the **Exchange Management Shell** application.

**Step 2** Enter the following command, where <Exchange server> is the IP address or fully qualified domain name of the Exchange server and <friendly name> is the friendly name that you chose for the Exchange server:

- **new-exchangecertificate -generaterequest -domainname <Exchange server> -friendlyname <friendly name>-path c:\csr.txt**

**Caution** The domain name for the Exchange server must be the IP address or the fully qualified domain name (recommended) so that the Unity Connection server can successfully ping the Exchange server. Otherwise, the calendar and contact integration may not function correctly.

**Step 3** Press **Enter**.

A Certificate Signing Request (CSR) file with the name Csr.txt is created in the root directory.

**Step 4** Send the CSR file to a Certification Authority (CA), which generates and sends back a new certificate.

**Note** You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange 2007 server.

**Step 5** Save the new certificate in a location that is accessible to the Exchange server on which you want to import the certificate.

**Step 6** On the Exchange Server, open the **Exchange Management Shell** application.

**Step 7** Enter the following command, where <path> is the full path of the new certificate that you received from the CA:

**import-exchangecertificate -path <path>**

**Step 8** Press **Enter**.

**Step 9** Enter the following command:

**dir cert:\localmachine\my | fl**

**Step 10** Press **Enter**.

**Step 11** Highlight the "thumbprint" property and press **Ctrl-C** to copy it to the clipboard.

**Step 12** If Unity Connection will be configured to use IMAP to access both email and calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 11:

**enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"**

If Unity Connection will not be configured to use IMAP but will be configured to use calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 11:

**enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"**

**Step 13** Press **Enter**.

**Step 14** If you want data transmitted as clear text, skip the remaining steps in this procedure and continue with the "Configuring Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration" section on page 36-6. Otherwise, open the **IIS Manager** application.

**Step 15** Go to **IIS > <server name> > Web Sites > Default Web Site**.

**Step 16** Right-click **Default Web Site** and select **Properties**.

**Step 17** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 18** Under **Secure Communications,** select **Edit**.

**Step 19** Check the **Require Secure Channel** check box.

**Step 20** Select **OK**.

**Step 21** In the **Properties** dialog box, select **OK**.

# Configuring Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration

Do the following procedure.

### To Configure Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **Exchange 2007 External Service Template**.

**Step 4** Check the **Enabled** check box to enable the calendar and contact integration.

**Step 5** In the **Display Name** field, enter a descriptive name.

**Step 6** In the **Server** field, enter the IP address or host name for the Exchange 2007 server.

**Step 7** In the **Authentication Mode** field, select the applicable setting to match the authentication mode that is used by the Exchange server.

**Step 8** In the **Security Transport** field, select the applicable setting:

- **None**—Unity Connection does not use a secure Unity Connection with the Exchange 2007 server.
- **SSL**—Unity Connection uses an SSL Unity Connection with the Exchange 2007 server.

**Step 9** If you selected "SSL" and you want Unity Connection to validate the Exchange 2007 server certificate, check the **Validate Server Certificate** check box.

Self-signed certificates cannot be validated. If you selected SSL and you are using self-signed certificates, do not check the **Validate Server Certificate** check box, or Unity Connection will not be able to access Exchange.

**Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of Server field. Otherwise, validation of the server certificate will fail.
The root certificate or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate must be installed as Unity Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

**Step 10** Under **Service Capabilities**, check the **User Access to Calendar and Personal Contacts** check box.

**Step 11** Select **Verify**. A message appears indicating whether the Cisco Unity Connection configuration has been successfully verified.

If the verification fails, confirm the configuration for Exchange 2007 and Cisco Unity Connection.

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

# Configuring Users for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection

Do the following procedure.

**Caution** Exchange 2007 must have a mailbox and Active Directory must have a user account for each Unity Connection user that you are configuring.

### To Configure Users for the Exchange 2007 Calendar and Contact Integration in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Note** If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**.

**Step 5** On the **New External Service Accounts** page, in the **External Service** field, select the display name that you entered in the "To Configure Cisco Unity Connection for the Exchange 2007 Calendar and Contact Integration" procedure on page 36-6.

**Step 6** In the **Email Address** field, enter the Exchange email address in Active Directory for the user.

**Step 7** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the Active Directory domain alias for the user is the same as the Unity Connection user alias. Unity Connection signs in the user with the Unity Connection user alias.
- **Use User ID Provided Below**—*(Recommended)* Enter the Active Directory domain alias for the user (useful when the User ID setting is different from the Unity Connection user alias). Unity Connection signs in the user with the setting in this field.

**Step 8** *(Only when the Use User ID Provided Below option is selected in Step 7)* In the User ID field, enter the User ID setting from Active Directory.

**Step 9** If known, in the **Password** field, enter the Active Directory domain password for the user. Unity Connection signs in the user with the setting in this field.

**Note** If you leave the Password field blank, users must sign in to Cisco Personal Communications Assistant and enter their password on the External Services Accounts page. For details, see the "Changing Your Cisco Unity Connection Passwords" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html.

**Step 10** Under **Service Capabilities**, check the **User Access to Calendar and Personal Contacts** check box.

**Note** A user can have only one external service that has the User Access to Calendar and Personal Contacts check box or the User Access to Calendar check box checked.

**Step 11** Select **Save**.

**Step 12** To check the calendar configuration for the user, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Exchange 2007, Active Directory, Cisco Unity Connection, and the Unity Connection user.

**Step 13** Repeat Step 2 through Step 12 for all remaining users.

# Testing the Exchange 2007 Calendar Integration in Cisco Unity Connection

Do the following procedure.

### To Test the Configuration for the Exchange 2007 Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to Outlook.

**Step 2** On the **Go** menu, select **Calendar**.

**Step 3** On the **File** menu, select **New > Meeting Request**.

**Step 4** Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

**Step 5** Select **Send**.

**Step 6** Sign in to the Cisco Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

**Step 7** If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Unity Connection reads the information about the Exchange 2007 meeting.

# Creating a Calendar and Contact Integration with Exchange 2003 in Cisco Unity Connection

If you have Exchange 2003 installed, you can integrate Cisco Unity Connection with Exchange 2003 so that users can do the following:

- Review upcoming meetings by phone or while using the Cisco Personal Communications Assistant (PCA).
- Import Active Directory contacts. The contact information can be used in rules that users create in the Personal Call Transfer Rules web tool and when users place outgoing calls by using voice commands.

For information on configuring calendar and contact integrations in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter and/or the "Configuring Cisco Unity Connection 10.x and Later and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

## Task List for Creating a Calendar and Contact Integration with Exchange 2003 in Cisco Unity Connection

1. Review the system requirements to confirm that all requirements for Exchange 2003 and the Cisco Unity Connection server have been met. See the "Requirements for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection" section on page 36-10.
2. Configure Exchange 2003. See the "Configuring Exchange 2003 for the Calendar and Contact Integration in Cisco Unity Connection" section on page 36-10.
3. Configure Unity Connection. See the "Configuring Cisco Unity Connection for the Exchange 2003 Calendar and Contact Integration" section on page 36-13.
4. *(When enabling personal call transfer rules only)* Verify that the users or templates are associated with a class of service that enables them to use the personal call transfer rules feature.
5. Configure the Unity Connection users. See the "Configuring Users for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection" section on page 36-14.
6. Test the calendar integration. See the "Testing the Exchange 2003 Calendar Integration in Cisco Unity Connection Do the following procedure." section on page 36-15.
7. To teach users how to use the Unity Connection calendar, refer them to the following:

- For listing, joining, and scheduling meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/phone/b_10xcucugphone.html.
- For importing Active Directory contacts, see the "Managing Your Personal Contacts" chapter of the *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/assistant/b_10xcucugasst.html.

- For using personal call transfer rules, see the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/pctr/b_10xcucugpctr.html.

# Requirements for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection

The calendar and contact integration with Exchange 2003 has the following requirements:

- Exchange 2003 as described in the "Requirements for Accessing Calendar Information for Meetings" and "Requirements for Accessing Exchange Contact Information" sections of *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring Exchange 2003 for the Calendar and Contact Integration in Cisco Unity Connection

Do the applicable procedures.

### To Create the Privileged Service Account for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection

**Step 1** On the Domain Controller, open **Active Directory Users and Computers**.

**Step 2** Right-click **Users** and select **New > User**.

**Step 3** Create a domain user account with alias **cucsvc**.

**Note** It is not necessary to create a mailbox for this user.

**Step 4** On the Exchange server, on the **Windows Start** menu, select **Programs > Microsoft Exchange > System Manager**.

**Step 5** Under **Servers,** right-click the server name and select **Properties**.

**Step 6** In the **Properties** dialog box, select the **Security** tab.

**Step 7** Select **Add** and add **cucsvc** (the alias for the domain account that you created in Step 3) to the list of accounts with permissions on the store.

**Step 8** Select **Check Names**.

**Step 9** Select **OK**.

**Step 10** In the list, select **cucsvc** (the alias for the domain account that you created in Step 3).

**Step 11** Set the permissions for the domain account alias to allow for **Receive As, Send As,** and **Administer Information Store**. Deny all other permissions.

**Step 12** In the **Properties** dialog box, select **OK**.

---

If you are not using SSL for access to the Exchange 2003 server, do the "To Configure Basic Access to Exchange 2003 for the Calendar and Contact Integration (Without SSL) in Cisco Unity Connection" procedure on page 36-11.

If you are using SSL for secure access to the Exchange 2003 server, do the "To Configure Secure Access to Exchange 2003 for the Calendar and Contact Integration (With SSL) in Cisco Unity Connection" procedure on page 36-12.

### To Configure Basic Access to Exchange 2003 for the Calendar and Contact Integration (Without SSL) in Cisco Unity Connection

---

**Step 1** On the Domain Controller, go to **Active Directory Users and Computers**.

**Step 2** Under **Users**, select all user accounts that have calendars that you want Unity Connection to access.

**Step 3** Right-click the highlighted users and select **Exchange Tasks**.

**Step 4** In the **Exchange Tasks** dialog box, select **Configure Exchange Features**.

**Step 5** Under **Protocols**, select **Outlook Web Access**.

**Step 6** Select the **Enable** icon.

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

**Step 8** Select **Finish**.

**Step 9** On the **Exchange** server, open the **Exchange System Manager** application.

**Step 10** Go to **Servers > <server name> > Protocols > HTTP > Exchange Virtual Server**.

**Step 11** Select the **Settings** tab.

**Step 12** Confirm that the **Enable Forms Based Authentication** check box is unchecked.

**Step 13** Select **OK**.

**Step 14** Go to **Servers > <server name> > Protocols > HTTP > Exchange Virtual Server > Exchange**.

**Step 15** Right-click **Exchange** and select **Properties**.

**Step 16** In the **Properties** dialog box, select the **Access** tab.

**Step 17** Confirm that the following check boxes are checked:

- Read
- Write
- Directory Browsing

**Step 18** Select **Authentication**.

**Step 19** Confirm that one or more of the following options are enabled:

- Basic
- Digest
- Integrated Windows Authentication

**Step 20** Select **OK**.

**Step 21** In the **Properties** dialog box, select **OK**.

**Step 22** Open the **IIS Manager** application.

**Step 23** Go to **IIS > <server name> > Web Sites > Default Web Site**.

**Step 24** Right-click **Default Web Site** and select **Properties**.

**Step 25** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 26** Under **Authentication and Access Control,** select **Edit**.

**Step 27** Confirm that the enabled authentication schemes match those that you enabled in Step 19.

**Step 28** Select **OK**.

**Step 29** In the **Properties** dialog box, select **OK**.

### To Configure Secure Access to Exchange 2003 for the Calendar and Contact Integration (With SSL) in Cisco Unity Connection

**Step 1** On the Exchange server, open the **IIS Manager** application.

**Step 2** Go to **IIS > Web Sites > Default Web Site**.

**Step 3** Right-click **Default Web Site** and select **Properties**.

**Step 4** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 5** Under **Secure Communications,** select **Server Certificate**.

**Step 6** Select **Next**.

**Step 7** Select **Create a New Certificate**.

**Note** If this option is not available, you must remove the existing certificate and do this step again.

**Step 8** Select **Prepare the Request Now, But Send It Later**.

**Step 9** Follow the prompts in the wizard to enter the applicable information for your organization.

**Caution** The “common name” for the Exchange server certificate must be the IP address or the fully qualified DNS name (recommended) of the Exchange server. Otherwise, the calendar and contact integration may not function correctly.

**Step 10** Save the **Certificate Signing Request (CSR)** as a file.

**Step 11** Send the CSR file to a Certification Authority (CA), which generates and sends back a new certificate.

**Note** You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange 2003 server.

**Step 12** Return to the **IIS Manager** application.

**Step 13** Go to **IIS > Web Sites > Default Web Site**.

**Step 14** Right-click **Default Web Site** and select **Properties**.

**Step 15** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 16** Under **Secure Communications,** select **Server Certificate**.

**Step 17** Select **Next**.

**Step 18** Select **Process the Pending Request and Install the Certificate** and select **Next**.

**Step 19** Browse to the local file system and select the new certificate that CA sent.

**Step 20** Select **Next**.

**Step 21** Confirm that the certificate information is valid and select **Next**.

**Step 22** Select **Finish**.

**Step 23** In the **Properties** dialog box, select **OK**.

**Step 24** Return to the **IIS Manager** application.

**Step 25** Go to **IIS > <sever name> > Web Sites > Default Web Site**.

**Step 26** Right-click **Default Web Site** and select **Properties**.

**Step 27** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 28** Under **Secure Communications,** select **Edit**.

**Step 29** Check the **Require Secure Channel** check box.

**Step 30** Select **OK**.

**Step 31** In the **Properties** dialog box, select **OK**.

# Configuring Cisco Unity Connection for the Exchange 2003 Calendar and Contact Integration

Do the following procedure.

### To Configure Cisco Unity Connection for the Exchange 2003 Calendar and Contact Integration

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **Exchange 2003 External Service Template**.

**Step 4** Check the **Enabled** check box to enable the external service.

When this check box is not checked, the integration with Exchange 2003 is disabled.

**Step 5** In the **Display Name** field, enter a descriptive name.

**Step 6** In the **Server** field, enter the IP address or host name for the Exchange 2003 server.

**Step 7** In the **Authentication Mode** field, select the applicable setting to match the authentication mode that is used by the Exchange server.

**Step 8** In the **Security Transport** field, select the applicable setting:

- **None**—Unity Connection does not use a secure Unity Connection with the Exchange 2003 server.
- **SSL**—Unity Connection uses an SSL Unity Connection with the Exchange 2003 server.

**Step 9** If you selected “SSL” and you want Unity Connection to validate the Exchange 2003 server certificate, check the **Validate Server Certificate** check box.

Self-signed certificates cannot be validated. If you selected SSL and you are using self-signed certificates, do not check the Validate Server Certificate check box, or Unity Connection will not be able to access Exchange.

**Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of Server field. Otherwise, validation of the server certificate will fail.

The root certificate or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate must be installed as Unity Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

**Step 10** In the **Alias** field, enter the Windows domain and alias for the privileged service account that Unity Connection uses to sign in to the Exchange 2003 server. (For example, enter "doman\alias").

This setting must match the user ID for the privileged service account that is configured in Exchange 2003.

**Step 11** In the **Password** field, enter the password for the privileged service account that Unity Connection uses to sign in to the Exchange 2003 server.

This setting must match the user password for the privileged service account that is configured in Exchange 2003.

**Step 12** Under **Service Capabilities**, check the **User Access to Calendar and Personal Contacts** check box.

**Step 13** Select **Save**.

**Step 14** To check the integration with Exchange 2003, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Exchange 2003 and Cisco Unity Connection.

# Configuring Users for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection

Do the following procedure.

**Note** Exchange 2003 must have a mailbox and Active Directory must have a user for each Unity Connection user that you are configuring.

### To Configure Users for the Exchange 2003 Calendar and Contact Integration in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Note** If the user alias does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Search**.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**.

**Step 5** On the **New External Service Accounts** page, in the **External Service** field, select the display name that you entered in the "To Configure Cisco Unity Connection for the Exchange 2003 Calendar and Contact Integration" procedure on page 36-13.

**Step 6** In the **Email Address** field, enter the primary SMTP address in Active Directory for the user.

**Step 7** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the User ID setting in Active Directory is the same as the Unity Connection user alias. Unity Connection signs in the user with the Unity Connection user alias.
- **Use User ID Provided Below**—Enter the User ID setting from Active Directory (useful when the User ID setting is different from the Unity Connection user alias). Unity Connection signs in the user with the setting in this field.

**Step 8** *(Only when the Use User ID Provided Below option is selected in Step 7)* In the User ID field, enter the User ID setting from Active Directory.

**Step 9** Under **Service Capabilities**, check the **User Access to Calendar and Personal Contacts** check box.

**Note** A user can have only one external service that has the User Access to Calendar and Personal Contacts check box or the User Access to Calendar check box checked.

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

**Step 11** To check the calendar configuration for the user, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Exchange 2003, Cisco Unity Connection, and the user.

**Step 12** Repeat Step 2 through Step 11 for all remaining users.

# Testing the Exchange 2003 Calendar Integration in Cisco Unity Connection Do the following procedure.

### To Test the Exchange 2003 Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to Outlook.

**Step 2** On the **Go** menu, select **Calendar**.

**Step 3** On the **File** menu, select **New > Meeting Request**.

**Step 4** Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

**Step 5** Select **Send**.

**Step 6** Sign in to the Unity Connection mailbox of the user that you invited to the Outlook meeting in Step 4.

**Step 7** If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Unity Connection reads the information about the Exchange 2003 meeting.

# Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace in Cisco Unity Connection

If you have Cisco Unified MeetingPlace installed, you can integrate Cisco Unity Connection with Cisco Unified MeetingPlace so that users can review upcoming meetings and join active meetings by phone.

For information on configuring calendar and contact integrations in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter and/or the "Configuring Cisco Unity Connection 10.x and Later and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

## Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace in Cisco Unity Connection

1. Review the system requirements to confirm that all requirements for Cisco Unified MeetingPlace and the Cisco Unity Connection server have been met. See the "Requirements for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection" section on page 36-16.
2. Configure Cisco Unified MeetingPlace. See the "Configuring Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection" section on page 36-17.
3. Configure Unity Connection. See the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration" section on page 36-18.
4. Configure the Unity Connection users. See the "Configuring Users for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection" section on page 36-19.
5. Test the calendar integration. See the "Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection" section on page 36-20.
6. To teach users how to list, join, and schedule meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/phone/b_10xcucugphone.html.

## Requirements for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection

The calendar integration with Cisco Unified MeetingPlace has the following requirements:

- Cisco Unified MeetingPlace as described in the "Requirements for Accessing Calendar Information for Meetings" section of *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection

Do the following procedure.

### To Configure Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to the Cisco Unified MeetingPlace Application Server as an administrator.

**Step 2** Select **User Configuration > User Profiles**.

**Step 3** Select **Add New**.

**Step 4** Enter the following values in the required fields to create a privileged service account:

| | |
|---|---|
| **First Name** | Leave this field blank. |
| **Last Name** | Enter **Cisco Unity Connection**. |
| **User ID** | Enter **cucsvc** or another user ID that you want. |
| **User Password** | Enter the applicable password. |
| **Profile Number** | Enter the applicable profile number. |
| **Profile Password** | Enter the applicable profile password. |
| **Type of User** | Select **System Administrator**. |

**Note** The values that you enter for the User ID, User Password, Profile Number, and Profile Password fields will be used in the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration" section on page 36-18.

**Step 5** Select **Save**.

**Step 6** Sign out of Cisco Unified MeetingPlace.

**Caution** If you do not sign out of Cisco Unified MeetingPlace, the test will fail in the "To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration in Cisco Unity Connection" procedure on page 36-18.

#### To Test the Cisco Unified MeetingPlace Configuration for the Calendar Integration in Cisco Unity Connection

**Step 1** In the Address field of a web browser, if SSL is not enabled, enter the following URL (where <server> is the IP address or host name of the Cisco Unified MeetingPlace server):

**http://<server>/webservices/services/meetingservice?wsdl**

If SSL is enabled, enter the following URL:

**https://<server>/webservices/services/meetingservice?wsdl**

**Step 2** Press **Enter**.

**Step 3** When prompted to sign in, enter the user ID and password for the privileged service account that you created in the "To Configure Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection" procedure on page 36-17.

The Cisco Unified MeetingPlace WSDL download page appears with the title "XFire Services."

# Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration

Do the following procedure.

#### To Configure Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **MeetingPlace 7.0/8.0 External Service Template**.

**Step 4** Check the **Enabled** check box to enable the external service.

When this check box is not checked, the integration with Cisco Unified MeetingPlace is disabled.

**Step 5** In the **Display Name** field, enter a descriptive name.

**Step 6** In the **Server** field, enter the IP address or host name for the Cisco Unified MeetingPlace server.

**Step 7** In the **Transfer Extension Dial String** field, enter the digits that Unity Connection must dial to transfer users on the phone to the opening greeting of Cisco Unified MeetingPlace server.

**Step 8** In the Security Transport field, select the applicable setting:

- **None**—Unity Connection does not use a secure Unity Connection with the Cisco Unified MeetingPlace server.
- **SSL**—Unity Connection uses an SSL Unity Connection with the Cisco Unified MeetingPlace server.

**Step 9** If you selected "SSL" and you want Unity Connection to validate the Cisco Unified MeetingPlace server certificate, check the **Validate Server Certificate** check box.

Self-signed certificates cannot be validated. If you selected SSL and you are using self-signed certificates, do not check the **Validate Server Certificate** check box, or Unity Connection will not be able to access Cisco Unified MeetingPlace.

**Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of Server field. Otherwise, validation of the server certificate will fail.

The root certificate or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate must be installed as Unity Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

**Step 10** In the **Alias** field, enter the alias for the privileged service account that Unity Connection uses to sign in to the Cisco Unified MeetingPlace server.

This setting must match the User ID setting for the privileged service account that you configured in the "Configuring Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection" section on page 36-17.

**Step 11** In the **Password** field, enter the password for the privileged service account that Unity Connection uses to sign in to the Cisco Unified MeetingPlace server.

This setting must match the User Password setting for the privileged service account that you configured in the "Configuring Cisco Unified MeetingPlace for the Calendar Integration in Cisco Unity Connection" section on page 36-17.

**Step 12** Under **Service Capabilities,** check the applicable check boxes:

- **User Access to Calendar**—Check this check box so that users can hear of their upcoming meetings by phone.
- **MeetingPlace Scheduling and Joining**—Check this check box so that users can schedule and join meetings.

**Step 13** Select **Save**.

**Step 14** To check the integration with Cisco Unified MeetingPlace, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace and Cisco Unity Connection.

# Configuring Users for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection

Do the following procedure.

**Caution** Cisco Unified MeetingPlace must have an end user for each Unity Connection user that you are configuring.

### To Configure Users for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**. The **New External Service Account** page appears.

**Step 5** In the **External Service** field, select the display name that you entered in the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Calendar Integration" section on page 36-18.

**Step 6** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the Cisco Unified MeetingPlace profile alias is the same as the Unity Connection user alias. Unity Connection signs in the user with the Unity Connection user alias. Cisco Unified MeetingPlace provides information on public and private meetings to the user.
- **Use Server Guest Account**—Unity Connection signs in the user as a guest, without using the Unity Connection user alias or the User ID setting. Cisco Unified MeetingPlace provides information only on public meetings to the user.
- **Use User ID Provided Below**—Enter the profile alias from Cisco Unified MeetingPlace (useful when the Cisco Unified MeetingPlace profile alias is different from the Unity Connection user alias). Unity Connection signs in the user with the setting in this field. Cisco Unified MeetingPlace provides information on public and private meetings to the user.

**Step 7** *(Only when the Use User ID Provided Below option is selected in Step 6)* In the User ID field, enter the User ID setting from Cisco Unified MeetingPlace.

**Step 8** Under **Service Capabilities,** check the applicable check boxes:

- **MeetingPlace Scheduling and Joining**—Check this check box so that the user can schedule and join meetings.
- **Primary Meeting Service**—If the MeetingPlace Scheduling and Joining check box is checked for two or more external services, check this check box so that Cisco Unified MeetingPlace meetings will be set up through this Cisco Unified MeetingPlace server. Uncheck this check box so that Cisco Unified MeetingPlace meetings will be set up through another server.

**Step 9** Select **Save**.

**Step 10** To check the calendar configuration for the user, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace, Cisco Unity Connection, and the user.

**Step 11** Repeat Step 2 through Step 10 for all remaining users.

# Testing the Calendar Integration for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection

Do the following procedure.

### To Test the Configuration for the Cisco Unified MeetingPlace Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to Cisco Unified MeetingPlace as an end user.

**Step 2** Select **Schedule**.

**Step 3** Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

**Step 4** Sign in to the Unity Connection mailbox of the user that you invited to the Cisco Unified MeetingPlace meeting in Step 3.

**Step 5** If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

**Step 6** When you hear the system announce the Cisco Unified MeetingPlace meeting that you just scheduled, either say **Join**, or press the applicable keys on the phone keypad to join the meeting.

# Creating a Calendar Integration with Cisco Unified MeetingPlace Express in Cisco Unity Connection

If you have Cisco Unified MeetingPlace Express installed, you can integrate Cisco Unity Connection with Cisco Unified MeetingPlace Express so that users can review upcoming meetings and join active meetings by phone or while using the Cisco Personal Communications Assistant (PCA).

Use the following task list to create a calendar integration.

For information on configuring calendar and contact integrations in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter and/or the "Configuring Cisco Unity Connection 10.x and Later and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

## Task List for Creating a Calendar Integration with Cisco Unified MeetingPlace Express in Cisco Unity Connection

1. Review the system requirements to confirm that all requirements for Cisco Unified MeetingPlace Express and the Cisco Unity Connection server have been met. See the "Requirements for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection" section on page 36-22.
2. Configure Cisco Unified MeetingPlace Express. See the "Configuring Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection" section on page 36-22.
3. Configure Unity Connection. See the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration" section on page 36-23.
4. Configure the Unity Connection users. See the "Configuring Users for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection" section on page 36-25.
5. Test the calendar integration. See the "Testing the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection" section on page 36-26.

6. To teach users how to list, join, and schedule meetings, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface (Release 10.x)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user/guide/phone/b_10xcucugphone.html.

# Requirements for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection

The calendar integration with Cisco Unified MeetingPlace Express has the following requirements:

- Cisco Unified MeetingPlace Express as described in the "Requirements for Accessing Calendar Information for Meetings" section of *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.
- Cisco Unity Connection installed as described in the *Installation Guide for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

# Configuring Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection

Do the following procedure.

### To Configure Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to Cisco Unified MeetingPlace Express and select **Administration**.

**Step 2** Select **User Configuration > User Profile Management**.

**Step 3** Select **Add New**.

**Step 4** Enter the following values in the required fields to create an API user:

| | |
|---|---|
| **First Name** | Leave this field blank. |
| **Last Name** | Enter **Cisco Unity Connection**. |
| **User ID** | Enter **cucsvc** or another user ID that you want. |
| **User Password** | Enter the applicable password. |
| **Profile Number** | Enter the applicable profile number. |
| **Type of User** | Select **API User**. |

**Note** The values that you enter for the User ID, User Password, and Profile Number fields will be used in the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration" section on page 36-23.

**Step 5** Select **Save**.

**Step 6** Sign out of Cisco Unified MeetingPlace Express.

**Caution** If you do not sign out of Cisco Unified MeetingPlace Express, the test will fail in the "To Test the Cisco Unified MeetingPlace Express Configuration for the Calendar Integration in Cisco Unity Connection" procedure on page 36-23.

### To Test the Cisco Unified MeetingPlace Express Configuration for the Calendar Integration in Cisco Unity Connection

**Step 1** In the Address field of a web browser, if SSL is not enabled, enter the following URL (where <server> is the IP address or host name of the Cisco Unified MeetingPlace Express server):

**http://<server>.com/webservices/services/meetingservice?wsdl**

If SSL is enabled, enter the following URL:

**https://<server>.com/webservices/services/meetingservice?wsdl**

**Step 2** Press **Enter**.

**Step 3** When prompted to sign in, enter the user ID and password for the API user that you entered in the "To Configure Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection" procedure on page 36-22.

The Cisco Unified MeetingPlace Express WSDL download page appears with the title "XFire Services."

# Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration

Do the following procedure.

### To Configure Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **MeetingPlace Express 2.0 External Service Template**.

**Step 4** Check the **Enabled** check box.

When this check box is not checked, the calendar integration with Cisco Unified MeetingPlace Express is disabled.

**Step 5** In the **Display Name** field, enter a descriptive name. For example, enter "Cisco Unified MeetingPlace Express calendar."

**Step 6** In the **Server** field, enter the IP address or host name for the Cisco Unified MeetingPlace Express server.

**Step 7** In the **Transfer Extension Dial String** field, enter the digits that Unity Connection must dial to transfer users on the phone to the opening greeting of Cisco Unified MeetingPlace Express server.

**Step 8** In the **Security Transport** field, select the applicable setting:

- **None**—Unity Connection does not use a secure Unity Connection with the Cisco Unified MeetingPlace Express server.
- **SSL**—Unity Connection uses an SSL Unity Connection with the Cisco Unified MeetingPlace Express server.

**Step 9** If you selected "SSL" and you want Unity Connection to validate the Cisco Unified MeetingPlace Express server certificate, check the **Validate Server Certificate** check box.

Self-signed certificates cannot be validated. If you selected SSL and you are using self-signed certificates, do not check the Validate Server Certificate check box, or Unity Connection will not be able to access Cisco Unified MeetingPlace Express.

**Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of Server field. Otherwise, validation of the server certificate will fail.

The root certificate or all certificates in a root certificate chain of the CA that signed the server certificate must be installed as Unity Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.

**Step 10** In the **Alias** field, enter the alias for the API user that Unity Connection uses to sign in to the Cisco Unified MeetingPlace Express server.

This setting must match the User ID setting for the API user that you configured in the "Configuring Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection" section on page 36-22.

**Step 11** In the **Password** field, enter the password for the API user that Unity Connection uses to sign in to the Cisco Unified MeetingPlace Express server.

This setting must match the User Password setting for the API user that you configured in the "Configuring Cisco Unified MeetingPlace Express for the Calendar Integration in Cisco Unity Connection" section on page 36-22.

**Step 12** Under Service Capabilities, check the applicable check boxes:

- **User Access to Calendar**—Check this check box so that users can hear their upcoming meetings on the phone.
- **MeetingPlace Scheduling and Joining**—Check this check box so that users can schedule and join meetings.

**Step 13** Select **Save**.

**Step 14** To check the integration with Cisco Unified MeetingPlace Express, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace Express and Cisco Unity Connection.

# Configuring Users for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection

Do the following procedure.

**Note** Cisco Unified MeetingPlace Express must have an end user for each Unity Connection user that you are configuring.

### To Configure Users for the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**. The **New External Service Accounts** page appears.

**Step 5** In the **External Service** field, select the display name that you entered in the "Configuring Cisco Unity Connection for the Cisco Unified MeetingPlace Express Calendar Integration" section on page 36-23.

**Step 6** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the Cisco Unified MeetingPlace Express profile alias is the same as the Unity Connection user alias. Unity Connection signs in the user with the Unity Connection user alias. Cisco Unified MeetingPlace Express provides information on public and private meetings to the user.
- **Use Server Guest Account**—Unity Connection signs in the user as a guest, without using the Unity Connection user alias or the User ID setting. Cisco Unified MeetingPlace Express provides information only on public meetings to the user.
- **Use User ID Provided Below**—Enter the profile alias from Cisco Unified MeetingPlace Express (useful when the Cisco Unified MeetingPlace Express profile alias is different from the Unity Connection user alias). Unity Connection signs in the user with the setting in this field. Cisco Unified MeetingPlace Express provides information on public and private meetings to the user.

**Step 7** *(Only when the Use User ID Provided Below option is selected in Step 6)* In the User ID field, enter the User ID setting from Cisco Unified MeetingPlace Express.

**Step 8** *(Only if enabled)* In the **User Profile Number** field, enter the **User ID** setting from Cisco Unified MeetingPlace Express. Unity Connection signs in the user with the setting in this field.

**Step 9** Under **Service Capabilities**, check the applicable check boxes:

- **User Access to Calendar**—Check this check box so that users can hear their upcoming meetings by phone.

**Note** A user can have only one external service that has the **User Access to Calendar and Personal Contacts check box or the User Access to Calendar** check box checked.

- **MeetingPlace Scheduling and Joining**—Check this check box so that the user can schedule and join meetings.

- **Primary Meeting Service**—If the **MeetingPlace Scheduling and Joining** check box is checked for two or more external services, check this check box so that Cisco Unified MeetingPlace Express meetings will be set up through this Cisco Unified MeetingPlace Express server. Uncheck this check box so that Cisco Unified MeetingPlace Express meetings will be set up through another server.

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

**Step 11** To check the calendar configuration for the user, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Cisco Unified MeetingPlace Express, Cisco Unity Connection, and the user.

**Step 12** Repeat Step 2 through Step 11 for all remaining users.

# Testing the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection

Do the following procedure.

### To Test the Cisco Unified MeetingPlace Express Calendar Integration in Cisco Unity Connection

**Step 1** Sign in to Cisco Unified MeetingPlace Express as an end user.

**Step 2** Select **Schedule**.

**Step 3** Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Cisco Unity Connection.

**Step 4** Sign in to the Unity Connection mailbox of the user that you invited to the Cisco Unified MeetingPlace Express meeting in Step 3.

**Step 5** If the user account is configured for speech access, say **Play Meetings**.

If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

**Step 6** When you hear the system announce the Cisco Unified MeetingPlace Express meeting that you just scheduled, either say **Join**, or press the applicable keys on the phone keypad to join the meeting.

# Configuring Service Parameters in Cisco Unity Connection 10.x

Service parameters for Cisco Unity Connection allow you to configure different services in Cisco Unified Serviceability. You can view a list of parameters and their descriptions by selecting the question mark button in the Service Parameter Configuration window. You can view the list with a particular parameter at the top by selecting that parameter.

If you turn off a service in Cisco Unified Serviceability, Unity Connection retains any updated service parameter values. If you start the service again, Unity Connection sets the service parameters to the changed values.

For more information about Cisco Unified Serviceability services, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

**Caution** Some changes to service parameters can cause system failure. We recommend that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (Cisco TAC) specifies the changes.

See the following sections:


- Configuring Service Parameters for a Cisco Unified Serviceability Service in Cisco Unity Connection 10.x, page 37-1
- Description of Service Parameters in Cisco Unity Connection 10.x, page 37-2


# Configuring Service Parameters for a Cisco Unified Serviceability Service in Cisco Unity Connection 10.x

Use the following procedure to configure the service parameters for a particular Cisco Unified Serviceability service.

### To Configure Service Parameters for a Cisco Unified Serviceability Service

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Service Parameters**.

**Step 2** On the **Service Parameters** page, in the **Server** list, select the name of the Cisco Unity Connection server.

**Step 3** In the **Service** list, select the service that contains the parameter that you want to update.

**Note** The **Service Parameters** page displays all services (active and not active).

**Step 4** Update the applicable parameter value. To set all service parameters for the service to the default values, select **Set to Default**.

To view a list of parameters and their descriptions, select the **?** button on the right side of the page.

**Step 5** Select **Save**.

# Description of Service Parameters in Cisco Unity Connection 10.x

Table 37-1 describes the service parameters for Cisco Unity Connection.

*Table 37-1 Service Parameter Descriptions*

| Service Parameter | Description |
|---|---|
| **Cisco AMC Service** | |
| Primary Collector | Specifies the Primary AMC (AlertMgr and Collector) server that collects clusterwide real-time information. Value must match one of the configured servers and, preferably, a server with no or minimal call processing.<br>This is a required field. |
| Failover Collector | Specifies the Failover AMC (AlertMgr and Collector) server. The server specified in this parameter is used to collect real-time data when the Primary AMC is down or unreachable. No data is collected if Failover Collector is not specified when Primary Collector is not active. |
| Data Collection Enabled | Determines whether collecting and alerting of real-time cluster information is enabled (True) or disabled (False).<br>This is a required field.<br>Default setting: True |
| Data Collection Polling Rate | Specifies the AMC collecting rate, in seconds.<br>This is a required field.<br>Default setting: 30<br>Minimum: 15<br>Maximum: 300<br>Unit: seconds |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| Server Synchronization Period | Specifies the amount of time, in seconds, that backup AMC (AlertMgr and Collector) waits at startup in order to determine if primary AMC is up and actively collecting. This parameter prevents backup AMC from assuming a collecting task prematurely.<br><br>This is a required field.<br><br>**Note** Restart the AMC service on the backup server for the parameter change to take effect.<br><br>Default setting: 60<br>Minimum: 15<br>Maximum: 300<br>Unit: seconds |
| RMI Registry Port Number | Specifies the port number to turn on RMI registry. This port is used for primary or backup AMC to locate other AMC, and for the RTMT servlet to find primary/backup AMC.<br><br>This is a required field.<br><br>**Note** Restart the AMC service for the parameter change to take effect.<br><br>Default setting: 1099<br>Minimum: 1024<br>Maximum: 65535 |
| RMI Object Port Number | Specifies the port number used for RMI remote object. This port is used for AMC to exchange data with other AMC as well as with RTMT servlet.<br><br>This is a required field.<br><br>**Note** Restart the AMC service for the parameter change to take effect.<br><br>Default setting: 1090<br>Minimum: 1024<br>Maximum: 65535 |
| AlertMgr Enabled | *(For AMC troubleshooting purpose only.)* Enables and disables the alerting (email/epage) feature.<br><br>This is a required field.<br><br>**Note** Restart the AMC service for the parameter change to take effect.<br><br>Default setting: True |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| Logger Enabled | *(For AMC troubleshooting purpose only.)* Enables and disables the logging feature (CSV files for generating reports).<br><br>This is a required field.<br><br>**Note** Restart the AMC service for the parameter change to take effect.<br><br>Default setting: True |
| **Cisco Database Layer Monitor Service** | |
| Maintenance Time | Specifies the hour to begin CDR database maintenance. Use this parameter in combination with the Maintenance Window parameter. For example, specifying 22 in this parameter means that the CDR maintenance would begin at 10 p.m. If the Maintenance Window parameter is set to 2, it means that CDR maintenance will run every hour from 10 p.m. to midnight. If both parameters are set to 24, CDR maintenance will run every hour all day long. During CDR maintenance, the system deletes the oldest CDRs and associated CMRs, so the maximum number of records, as specified in the Max CDR Records parameter, is maintained. Also during maintenance, the system issues an alarm if the CDR file count exceeds 200, and checks for replication links between servers that have been broken and tries to reinitialize them.<br><br>This is a required field.<br><br>Default setting: 24<br>Minimum: 1<br>Maximum: 24<br>Unit: hours |
| Maintenance Window | Specifies the window of time during which CDR maintenance is performed on an hourly basis. For example, if this parameter is set to 12, CDR maintenance will run every hour for 12 hours, starting at the time that is specified in the Maintenance Time parameter. For example, if the Maintenance Time parameter is set to 7, and this parameter is set to 12, CDR maintenance will begin at 7 a.m. and run every hour until 7 p.m. If both parameters are set to 24, CDR maintenance will run every hour all day long. During CDR maintenance, the system deletes the oldest CDRs and associated CMRs, so the maximum number of records, as specified in the Max CDR Records parameter, is maintained. Also, during maintenance, the system issues an alarm if the CDR file count exceeds 200, and checks for replication links between servers that have been broken and tries to reinitialize them.<br><br>This is a required field.<br><br>Default setting: 2<br>Minimum: 1<br>Maximum: 24<br>Unit: hours |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| Table Out of Sync Detection | When set to On, collects Database Replication Status summary every day during the Maintenance window and compares the output of three consecutive days to determine if there are tables that have been out of sync for all three days. If that is the case, it will trigger an alert. This parameter, by default, is set to Off and is run at time specified in Maintenance Time parameter.<br>This is a required field.<br>Default: Off |
| MaintenanceTaskTrace | Sets the Maintenance Task trace. You must turn on this parameter to get a performance counter trace from the Maintenance Task.<br>This is a required field.<br>Default setting: Off |
| **Cisco DirSync** | |
| Maximum Number of Agreements | Specifies the maximum number of LDAP directories (also known as agreements) that can be configured in the LDAP Directory window in Cisco Unified CM Administration (System > LDAP > LDAP Directory). Creating more than one LDAP directory helps in synchronizing users from more than one search base.<br>This is a required field.<br>**Note** You must restart the Cisco DirSync service for changes to this parameter to take effect.<br>Default setting: 5<br>Minimum: 1<br>Maximum: 5 |
| Maximum Number of Hosts | Specifies the maximum number of LDAP host names that can be configured for failover purposes.<br>This is a required field.<br>**Note** You must restart the Cisco DirSync service for changes to this parameter to take effect.<br>Default setting: 3<br>Minimum: 1<br>Maximum: 3 |
| Retry Delay on Host Failure (secs) | Specifies the number of seconds to delay before retrying the Unity Connection to the first LDAP server (host name) that is configured in Cisco Unified CM Administration. After a Unity Connection failure, the system tries three times to reconnect to the same host. When the third attempt is also unsuccessful, the system attempts to connect to the next host name in the list in hierarchical order.<br>This is a required field.<br>Default setting: 5<br>Minimum: 5<br>Maximum: 60 |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| Retry Delay on HostList Failure (mins) | Specifies the number of minutes to delay before retrying every LDAP server (host names) that is configured in Cisco Unified CM Administration. Unity Connection to LDAP servers are retried in the order they appear in Unified CM Administration and three Unity Connection attempts are made based on the delay interval specified in the Retry Delay On Host Failure service parameter. When all three Unity Connection attempts fail to result in a Unity Connection to the LDAP server, the next LDAP server in the list is tried. If the system is unable to connect to any of the servers in the list, an error gets logged and the system waits until the next sync interval before retrying to connect starting with the first server in the list.<br><br>This is a required field.<br><br>Default setting: 10<br>Minimum: 10<br>Maximum: 120 |
| LDAP Unity Connection Timeout (secs) | Specifies the number of seconds allowed for establishing the LDAP Unity Connection. The LDAP service provider aborts the Unity Connection attempt if a Unity Connection cannot be established in the specified amount of time.<br><br>This is a required field.<br><br>Default setting: 5<br>Minimum: 1<br>Maximum: 60 |
| Delayed Sync Start Time (mins) | Specifies the delay in starting the directory synchronization process after the Cisco DirSync service starts. Directory synchronization ensures that the users in the LDAP server are copied to the Cisco Unified Communications Manager database.<br><br>This is a required field.<br><br>**Note** You must restart the Cisco Tomcat service for changes to this parameter to take effect.<br><br>Default setting: 5<br>Minimum: 5<br>Maximum: 60 |
| **Cisco RIS Data Collector Parameters** | |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| RIS Cluster TCP Port | Specifies specifies the static TCP port that the Cisco RIS Data Collector services in the cluster use to communicate with each other. Note: You must restart the Cisco RIS Data Collector service on each node in the cluster for the parameter change to take effect.<br><br>This is a required field.<br><br>**Note** Restart the Cisco RIS Data Collector service on each node in the cluster for the parameter change to take effect.<br><br>Default setting: 2555<br>Minimum: 1024<br>Maximum: 65535 |
| RIS Client TCP Port | Specifies the static TCP port that the RIS clients use to communicate with the Cisco RIS Data Collector services in the cluster. Note: You must restart Cisco Database Layer Monitor service, and the Cisco the RIS Data Collector service on each node in the cluster for the parameter change to take effect.<br><br>This is a required field.<br><br>**Note** Restart Cisco Database Layer Monitor service, and the Cisco RIS Data Collector services on each node in the cluster for the parameter change to take effect.<br><br>Default setting: 2556<br>Minimum: 1024<br>Maximum: 65535 |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| RIS Client Timeout | the time, in seconds, that a RIS client will wait for a reply from the Cisco RIS Data Collector service. The RIS Data Collector service running on each node internally distributes 90 percent of the value specified in this parameter. To set this parameter correctly for a cluster with multiple nodes, specify a value that is 4 times (or more) the number of nodes that are running the RIS Data Collector service in your cluster. For example, if you have 7 nodes in the cluster that are running the RIS Data Collector service, set this value to 28 or higher. For a cluster with two nodes, set this parameter to 10, the minimum allowed value (or higher).<br><br>Choosing a higher value helps ensure that the RIS Data Collector service on one node has enough time to receive a reply from the RIS Data Collector service on another node. The time needed for a reply can vary based on factors such as the node's processor speed, number of devices registered to the node, amount of server memory, the volume of calls, and other performance-affecting factors. NOTE: If the value in this parameter is set lower than the recommended 4x nodes value, Unified CM will internally increase the value to allow that needed minimum number of seconds per node. Actual response might be shorter; this value only indicates the maximum allowed time so choosing a higher value will not negatively affect performance.<br><br>This is a required field.<br><br>Default setting: 30<br>Minimum: 10<br>Maximum: 1000<br>Unit: seconds |
| RIS Cleanup Time of the Day | Specifies the time of the day that the RIS database will be cleaned up to remove any unused, old device information. During this time, the NumofRegistrationAttempts performance counters for all devices reset to 0.<br><br>This is a required field.<br><br>Default setting: 22:00<br>Maximum length: 5<br>Allowed values: Specify time in HH:mm format (for example 06:11).<br>Unit: hours:minutes |
| RIS Unused Cisco CallManager Device Store Period | Specifies specifies the RIS database information storage period for any unregistered or rejected device information from the Cisco CallManager service. After the time specified in this parameter expires, Cisco CallManager removes the expired entries during the next RIS database cleanup time (specified in the RIS Cleanup Time of the Day parameter).<br><br>This is a required field.<br><br>Default setting: 3<br>Minimum: 1<br>Maximum: 30<br>Unit: days |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| RIS Unused CTI Records Storage Period | Specifies the RIS database information storage period for any closed provider, device, or line information from the CTI Manager. After the time specified in this parameter expires, Cisco CTI Manager removes the expired entries during the next RIS database cleanup time (specified in the RIS Cleanup Time of the Day parameter).<br><br>This is a required field.<br><br>Default setting: 1<br>Minimum: 0<br>Maximum: 5<br>Unit: days |
| RIS Maximum Number of Unused CTI Records | Specifies the maximum number of records for closed CTI providers, devices, and lines that will be kept in the RIS database. After the limit specified in this parameter is reached, Cisco CTI Manager does not save any new record for unused CTI providers, devices, or lines to the RIS database.<br><br>This is a required field.<br><br>Default setting: 3000<br>Minimum: 0<br>Maximum: 5000<br>Unit: records |
| TLC Throttling Enabled | Enables or disables Trace and Log Central throttling behavior.<br><br>This is a required field.<br><br>Default setting: True |
| TLC Throttling IOWait Goal | Specifies the system IOWait percentage that TLC throttles itself toward.<br><br>This is a required field.<br><br>Default setting: 10<br>Minimum: 10<br>Maximum: 40 |
| TLC Throttling CPU Goal | Specifies the system CPU utilization percentage that TLC throttles itself toward.<br><br>This is a required field.<br><br>Default setting: 80<br>Minimum: 65<br>Maximum: 90 |
| TLC Throttling Polling Delay | Specifies the minimum delay in milliseconds between IO wait and CPU usage polls for the purpose of trace collection throttling.<br><br>This is a required field.<br><br>Default setting: 250<br>Minimum: 200<br>Maximum: 2000 |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| TLC Throttling SFTP Maximum Delay | Specifies the maximum time an SFTP transfer is paused in order to prevent timeouts.<br><br>This is a required field.<br><br>Default setting: 5000<br>Minimum: 1000<br>Maximum: 10000 |
| Maximum Number of Processes and Threads | Specifies the maximum number of Processes and Threads running on the machine. If the total number of Processes and Threads on the machine has exceeded this maximum number, SystemAccess sends alarm TotalProcessesThreadsExceededThresholdStart and the corresponding alert is generated.<br><br>This is a required field.<br><br>Default setting: 2000<br>Minimum: 1000<br>Maximum: 3000 |
| Enable Logging | Determines whether collecting and logging of troubleshooting perfmon data is enabled (True) or disabled (False).<br><br>This is a required field.<br><br>Default setting: True |
| Polling Rate | Specifies the troubleshooting perfmon data polling rate, in seconds.<br><br>This is a required field.<br><br>Default setting: 15<br>Minimum: 5<br>Maximum: 300<br>Unit: seconds |
| Maximum No. of Files | Specifies the maximum number of troubleshooting perfmon log files that are saved on disk. If the "Maximum No. of Files" is set to a large number, it is recommended that the "Maximum File Size" be reduced.<br><br>This is a required field.<br><br>**Note** If this value is reduced, excessive log files with the oldest time stamp will be deleted if Troubleshooting Perfmon Data Logging is enabled and RISDC is turned on. If desired, please save these files first before changing Maximum No. of Files.<br><br>Default setting: 50<br>Minimum: 1<br>Maximum: 100 |

*Table 37-1 Service Parameter Descriptions (continued)*

| Service Parameter | Description |
|---|---|
| Maximum File Size (MB) | Specifies the maximum file size, in megabytes, in each troubleshooting perfmon log file before the next file is started. If the "Maximum File Size" is set to a large number, it is recommended that the "Maximum No. of Files" be reduced.<br><br>This is a required field.<br><br>Default setting: 5<br>Minimum: 1<br>Maximum: 500 |
| **Cisco Serviceability Reporter** | |
| RTMT Reporter Designated Node | Specifies specifies the designated node on which RTMTReporter runs. It is desirable that this node is a non-callprocessing node since RTMTReporter service is CPU-intensive. This field will be automatically filled in with the local node IP at which Reporter is first turned on.<br><br>This is a required field. |
| RTMT Report Generation Time | Specifies the number of minutes after midnight (00:00hrs) when the Real-Time Monitoring Tool, (RTMT) reports are generated. To reduce any impact to call processing, run non-real-time reports during non-production hours.<br><br>This is a required field.<br><br>Default setting: 30<br>Minimum: 0<br>Maximum: 1200 |
| RTMT Report Deletion Age | Specifies the number of days that must elapse before reports are deleted. For example, if this parameter is set to 7, reports that were generated seven days ago get deleted on the eighth day. A value of 0 disables report generation, and any existing reports get deleted.<br><br>This is a required field.<br><br>Default setting: 7<br>Minimum: 0<br>Maximum: 30 |

# Configuring Enterprise Parameters in Cisco Unity Connection 10.x

Enterprise parameters for Cisco Unity Connection provide default settings that apply to all services in Cisco Unified Serviceability.

You cannot add or delete enterprise parameters, but you can use the procedure in this section to update the existing enterprise parameters.

**Note** Many of the enterprise parameters rarely require change. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (Cisco TAC) specifies the change.

See the following sections:


- Configuring Enterprise Parameters for Cisco Unified Serviceability Services in Cisco Unity Connection 10.x, page 38-1
- Description of Enterprise Parameters in Cisco Unity Connection 10.x, page 38-2


## Configuring Enterprise Parameters for Cisco Unified Serviceability Services in Cisco Unity Connection 10.x

Use the following procedure to configure enterprise parameters for Cisco Unified Serviceability services.

### To Configure Enterprise Parameters for Cisco Unified Serviceability Services

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Enterprise Parameters**.

**Step 2** On the **Enterprise Parameters Configuration** page, enter the applicable settings. To set all service parameters to the default values, select **Set to Default**.

To view a list of enterprise parameters and their descriptions, select the **?** button on the right side of the page.

**Step 3** Select **Save**.

# Description of Enterprise Parameters in Cisco Unity Connection 10.x

Table 38-1 describes the enterprise parameters available in Cisco Unity Connection.

*Table 38-1 Enterprise Parameter Descriptions*

| Enterprise Parameter | Description |
|---|---|
| Max Number of Device Level Trace | Specifies how many devices can be traced concurrently if device name-based trace is selected in Trace Configuration in Cisco Unified Serviceability.<br>This is a required field.<br>Default setting: 12<br>Minimum: 0<br>Maximum: 256 |
| **Localization Parameters** | |
| Default Network Locale | Specifies the default network locale for tones and cadences. The chosen network locale applies to all gateways and phones that do not have the network locale set at the device or device pool level.<br>This is a required field.<br>**Note** Make sure that the chosen network locale is installed and supported for all gateways and phones. See the product documentation, if necessary. Reset all devices for the parameter change to take effect.<br>Default setting: United States |
| Default User Locale | Specifies the default user locale for language selection. Not all locales are supported by all models. For models that do not support this setting, set their locale explicitly to something they support.<br>This is a required field.<br>**Note** Reset all devices for the parameter change to take effect.<br>Default setting: English United States |
| **Prepare Cluster for Rollback** | |
| Prepare Cluster for Rollback to Pre 9.0 | If a Cisco Unity Connection cluster is configured and was upgraded, specifies whether the previous version of Unity Connection was release 7.x.<br>This is a required field.<br>Default setting: False |
| **Trace Parameters** | |
| File Close Thread Flag | Enables the use of separate threads to close trace files. This may improve the performance of the system at the end of a trace file.<br>This is a required field.<br>Default setting: True |

*Table 38-1 Enterprise Parameter Descriptions (continued)*

| Enterprise Parameter | Description |
|---|---|
| FileCloseThreadQueueWaterMark | Defines the high-water mark after which the separate thread used to close trace files stops accepting trace files to close; the trace file is then closed without the use of a separate thread.<br><br>This is a required field.<br><br>Default setting: 100<br>Minimum: 0<br>Maximum: 500 |
| **Clusterwide Domain Configuration Parameters** | |
| Organization Top Level Domain | Defines the top level domain for the organization (for example, cisco.com).<br><br>Maximum length: 255<br>Allowed values: Provide a valid domain (for example, cisco.com) with up to 255 of the following characters: any upper or lower case letter (a-zA-Z), any number (0-9), the hyphen (-), or the dot (.) The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om is an example of an invalid domain. |
| Cluster Fully Qualified Domain Name | Defines one or more Fully Qualified Domain Names (FQDN) for this cluster. Multiple FQDNs must be separated by a space. Wildcards can be specified within an FQDN using an asterisk (*). Examples are cluster-1.rtp.cisco.com and *.cisco.com. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter are recognized as a request destined for this cluster and/or devices attached to it.<br><br>Maximum length: 255<br>Allowed values: Provide one or more fully qualified domain names (FQDN), or partial FQDNs using the * wildcard (for example, cluster-1.cisco.com or *.cisco.com). Multiple FQDNs must be separated by a space. The following characters are allowed: any upper or lower case letter (a-zA-Z), any number (0-9), hyphen (-), asterisk (*), or dot (.) The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om serves as an example of an invalid domain. |
| **Cisco Support Use** | |
| Cisco Support Use 1 | Is used by Cisco TAC only.<br><br>Maximum length: 10 |
| Cisco Support Use 2 | Is used by Cisco Technical Support only.<br><br>Maximum length: 10 |
| **Cisco Syslog Agent** | |

*Table 38-1 Enterprise Parameter Descriptions (continued)*

| Enterprise Parameter | Description |
|---|---|
| Remote Syslog Server Name 1 to Remote Syslog Server Name 5 | Enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. You can configure upto five Remote Syslog Servers to accept Syslog messages. If a server name is not specified, Cisco Unified Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server.<br><br>Maximum length: 255<br>Allowed values: Provide a valid remote syslog server name with the following characters: A-Z, a-z, 0-9, ., - |
| Syslog Severity for Remote Syslog Messages | Select the desired Syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to remote syslog. If a remote server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.<br><br>This is a required field.<br><br>Default setting: Error |
| **CUCReports Parameters** | |
| Report Socket Unity Connection Timeout | Specifies the maximum number of seconds used when attempting to establish a Unity Connection with another server. Increase this time if Unity Connection issues are experienced on a slow network.<br><br>This is a required field.<br><br>Default setting: 10<br>Minimum: 5<br>Maximum: 120 |
| Report Socket Read Timeout | Specifies the maximum number of seconds used when reading data from another server. Increase this time if Unity Connection issues are experienced on a slow network.<br><br>This is a required field.<br><br>Default setting: 60<br>Minimum: 5<br>Maximum: 600 |

# Installing Plugins in Cisco Unity Connection 10.x

Application plugins extend the functionality of Cisco Unity Connection. For example, the Real-Time Monitoring Tool (RTMT) allows you to monitor the health of the system remotely through tools such as performance-monitoring counters and the Port Monitor.

Do the following procedure.

**Note** Before you install any plugins, you must disable all intrusion detection or antivirus services that run on the server where you will install the plugin.

### To Install a Plugin

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Plugins**.

**Step 2** On the **Search Plugins** page, select **Find**.

**Step 3** For the plugin that you want to install, select **Download**.

**Step 4** Follow the on-screen instructions for installing the plugin.

# Managing Descriptions of Message Attachments in Cisco Unity Connection 10.x

When Cisco Unity Connection is integrated with a third-party message store, Unity Connection uses Text to Speech (TTS) to describe message attachments for users who check their messages on the phone. For example, an attachment with the extension .jpg is described as “an image.”

You can change the description of the attachments, add descriptions for attachments, and delete descriptions of attachments.

See the following sections:


- Adding a Description of a Message Attachment in Cisco Unity Connection 10.x, page 40-1
- Changing a Description of a Message Attachment in Cisco Unity Connection 10.x, page 40-2
- Deleting a Description of a Message Attachment in Cisco Unity Connection 10.x, page 40-2


## Adding a Description of a Message Attachment in Cisco Unity Connection 10.x

You can add a description of message attachments that Cisco Unity Connection reads when users check their messages by phone.

### To Add a Description of a Message Attachment

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Attachment Descriptions**.

**Step 2** On the **Search TTS Descriptions of Message Attachments** page, in the **Language** list, select the language for which you want to add a description of a message attachment.

**Note** The list of languages depends on the languages (locales) that are installed on Unity Connection.

**Step 3** Select **Add New**.

**Step 4** On the **New TTS Description of Message Attachments** page, enter a file extension in the **File Extension** field.

You must enter a period at the beginning of the file extension. Otherwise, you cannot add the description of the message attachment.

**Step 5** In the **Description** field, enter the description that you want for the message attachment.

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

# Changing a Description of a Message Attachment in Cisco Unity Connection 10.x

You can change a description of message attachments that Cisco Unity Connection reads when users check their messages by phone.

### To Change a Description of a Message Attachment

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Attachment Descriptions**.

**Step 2** On the **Search TTS Descriptions of Message Attachments** page, in the **Language** list, select the language for which you want to change a description of a message attachment.

**Note** The list of languages depends on the languages (locales) that are installed on Unity Connection.

**Step 3** In the **Extension** column, select the extension for the attachment description that you want to change.

**Step 4** On the **Edit TTS Descriptions of Message Attachments** page, enter a file extension in the **File Extension** field.

You must enter a period at the beginning of the file extension. Otherwise, you cannot add the description of the message attachment.

**Step 5** In the **Description** field, enter the description that you want.

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

# Deleting a Description of a Message Attachment in Cisco Unity Connection 10.x

You can remove a description of a message attachment that you do not want Cisco Unity Connection to read when users check their messages on the phone.

### To Delete a Description of a Message Attachment

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Attachment Descriptions**.

**Step 2** On the **Search TTS Descriptions of Message Attachments** page, in the **Language** list, select the language for which you want to delete a description of a message attachment.

**Note** The list of languages depends on the languages (locales) that are installed on Unity Connection.

**Step 3** Check the check box next to the extension for the attachment description that you want to delete.

**Step 4** Select **Delete Selected**.

**Step 5** When prompted to confirm the deletion, select **OK**.

# Setting Up Phone View in Cisco Unity Connection 10.x

The Phone View feature allows users to see search results on the LCD screens of their Cisco IP phones when they use the **Find Message** or the **Display Message** menu. When Phone View is enabled, Cisco Unity Connection users can search for the following types of voice messages:

- All new messages
- All messages
- Messages from a particular user
- Messages from all outside callers
- Messages from a particular outside caller

Phone View works only with Cisco Unified Communications Manager phone systems, and only with certain Cisco IP phones. See the applicable requirements documentation for detailed information in *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.

Phone View can be used with either the touchtone or the voice-recognition version of the phone conversation.

To set up Phone View, complete the following tasks in the order presented:

1. Create a CTI application user in Cisco Unified CM, and associate the applicable user devices with this user. See the applicable procedure for your version of Cisco Unified CM:
   - To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 6.x and Later), page 41-2
   - To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 5.x), page 41-2
2. Enable Phone View for a phone system integration on Cisco Unity Connection. See the "To Enable Phone View for a Phone System (Cisco Unified Communications Manager Only)" procedure on page 41-3.
3. Enable Phone View for users. See the "Phone View in Cisco Unity Connection 10.x" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

### To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 6.x and Later)

**Step 1** In Cisco Unified CM Administration, select **User Management > Application User**.

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

**Step 3** On the **Application User Configuration** page, do the following substeps to create a CTI user account that has access to all user phones for Phone View:

a. In the **User ID** field, enter a unique name for the application user. For example, enter "PhoneViewUser."

b. In the **password** field, enter a password for the application user.

c. In the **Confirm Password** field, re-enter the password that you entered in Step 3b.

d. Under **Device Information**, to the right of the **Available Devices** field, select **Find More Phones**.

e. On the **Find and List Phones** page, select the phones on which you want to enable Phone View and select **Add Selected**.

f. On the **Application User Configuration** page, confirm that the phones on which you want to enable **Phone View appear in the Controlled Devices** field so that the phones are associated with the application user.

For any phones that you selected in Step 3e. and that appear in the **Available Devices** field, select the applicable phones and select the **Down** arrow below the field to move the phones to the **Controlled Devices** field.

g. Under **Permissions Information**, select **Add to User Group**.

h. On the **Find and List User Groups** page, check the **Standard CCM Admin Users** check box and select **Add Selected**.

i. On the **Application User Configuration** page, select **Save**.

j. Under **Application User Information,** select **Edit Credential**.

k. On the **Credential Configuration** page, confirm that the **User Must Change at Next Sign-In** check box is not checked and select **Save**.

**Step 4** Continue with the "To Enable Phone View for a Phone System (Cisco Unified Communications Manager Only)" section on page 41-3.

### To Configure Cisco Unified Communications Manager for Phone View (Cisco Unified CM 5.x)

**Step 1** In Cisco Unified Communications Manager Administration, select **User Management > Application User**.

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

**Step 3** On the **Application User Configuration** page, do the following sub-steps to create an application user account that has access to all subscriber phones for Phone View:

a. In the **User ID** field, enter the name of the a unique name for the application user. For example, enter "PhoneViewUser."

b. In the **password f**ield, enter a password for the application user.

c. In the **Confirm Password** field, re-enter the password that you entered in Step 3b.

d. Under **Device Information**, to the right of the **Available Devices** field, select **Find More Phones**.

e. On the **Find and List Phones** page, select the phones on which you want to enable Phone View and select **Add Selected**.

f. On the **Application User Configuration** page, confirm that the phones on which you want to enable **Phone View appear in the Controlled Devices** field so that the phones are associated with the application user.

   For any phones that you selected in Step 3e. and that appear in the Available Devices field, select the applicable phones and select the **Down** arrow below the field to move the phones to the **Controlled Devices** field.

g. On the **Application User Configuration** page, select **Save**.

h. Select **User Management > User Group**.

i. On the **Find and List User Groups,** select **Standard CCM Admin Users**.

j. On the **User Group Configuration** page, select **Add Application Users to Group**.

k. On the **Find and List Application User** page, check the check box for the application user that you created in Step Step 3g.

l. Select **Add Selected**.

**Step 4** Continue with the "To Enable Phone View for a Phone System (Cisco Unified Communications Manager Only)" section on page 41-3.

### To Enable Phone View for a Phone System (Cisco Unified Communications Manager Only)

**Step 1** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

**Step 2** Find the Cisco Unified Communications Manager phone system that you want to change.

**Step 3** Under **Phone View Settings**, check the **Enable Phone View** check box.

**Step 4** In the **CTI Phone Access User Name** field, enter the name of the application user that you created in Cisco Unified Communications Manager for the Phone View features. Note that the username is case-sensitive.

**Step 5** In the **CTI Phone Access Password** field, enter the password for the application user.

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

# Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 10.x

See the following sections:


- About Text-to-Speech Access to Exchange Emails in Cisco Unity Connection, page 42-1
- Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection, page 42-1
- Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection, page 42-6


For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

## About Text-to-Speech Access to Exchange Emails in Cisco Unity Connection

When Cisco Unity Connection is configured to connect to an external message store (a message store other than Cisco Unity Connection), users can hear their emails read to them when they sign in to Cisco Unity Connection by phone. In this chapter, you configure Microsoft Exchange and Cisco Unity Connection so that licensed users can listen to emails.

**Note** Text-to-speech over Exchange 2007 and Exchange 2010 supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Unity Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrug051.html.

## Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection

If you configure Cisco Unity Connection to integrate with Exchange 2007, users can access emails in an Exchange 2007 message store.

See the following sections:


- Task List for Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection, page 42-2
- Enabling IMAP Access to Exchange in Cisco Unity Connection, page 42-2
- Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only), page 42-3
- Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection, page 42-4
- Configuring Users for the External Services in Cisco Unity Connection, page 42-5


For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

# Task List for Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection

To enable users to access emails in an Exchange 2007 message store, complete the following tasks in the order presented.

1. Enable IMAP Access to Exchange. See the "Enabling IMAP Access to Exchange in Cisco Unity Connection" section on page 42-2.
2. Create and install an SSL server certificate on each Exchange server on which you want to access email messages. See the "Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)" section on page 42-3.
3. Create Unity Connection external services. See the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 42-4.
4. Configure the users for the external services. See the "Configuring Users for the External Services in Cisco Unity Connection" section on page 42-5.
5. Associate users with a class of service that offers a license to access the TTS feature, and enables them to use it.
6. For each user, create an external service account in Unity Connection that specifies the Exchange server on which the mailbox for the user is stored. This enables users to access their email when they sign in to Unity Connection by phone.

# Enabling IMAP Access to Exchange in Cisco Unity Connection

Cisco Unity Connection uses the IMAP protocol to access emails in Exchange so that the messages can be played by using TTS. By default, Exchange is not configured to allow IMAP access to messages. Do the following procedure to enable IMAP access on each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

### To Enable IMAP Access to Exchange in Cisco Unity Connection

**Step 1** On an Exchange server that contains emails that you want licensed Unity Connection users to be able to access, sign in to Windows by using an account that is a member of the local Administrators group.

**Step 2** On the **Windows Start** menu, select **Administrative Tools > Services**.

**Step 3** In the right pane, find the **Microsoft Exchange IMAP4** service.

**Step 4** If the value of the **Status** column is **Started** and the value of the Startup Type column is **Automatic**, skip to Step 9.

If the values are different, double-click **Microsoft Exchange IMAP4**.

**Step 5** In the **Microsoft Exchange IMAP4 Properties** dialog box, if **Startup Type is not Automatic**, change it to **Automatic**.

**Step 6** If **Service Status** is not Started, select **Start**.

**Step 7** Select **OK** to close the **Microsoft Exchange IMAP4 Properties** dialog box.

**Step 8** Close the **Services MMC.**

**Step 9** Repeat Step 1 through Step 8 on each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

# Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)

### To Configure Secure IMAP with SSL and Enable the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)

**Step 1** On the Exchange Server, open the **Exchange Management Shell** application.

**Step 2** Enter the following command, where <Exchange server> is the IP address or host name of the Exchange server and <friendly name> is the friendly name that you select for the Exchange server:

**new-exchangecertificate -generaterequest -domainname <Exchange server> -friendlyname <friendly name>-path c:\csr.txt**

**Caution** The domain name for the Exchange server must be the IP address or the fully qualified DNS name (recommended) so that the Unity Connection server can successfully ping the Exchange server. Otherwise, users may not be able to access their emails in the external message store.

**Step 3** Press **Enter**. A Certificate Signing Request (CSR) file with the name Csr.txt is created in the root directory.

**Step 4** Send the CSR file to a Certification Authority (CA), which will generate and send back a new certificate.

**Note** You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange 2007 server.

**Step 5** Enter the following command, where <path> is the location of the directory where the CA will save the new server certificate:

**import-exchangecertificate -path <path>**

**Step 6** Press **Enter**.

**Step 7** Enter the following command:

**dir cert:\localmachine\my | fl**

**Step 8** Press **Enter**.

**Step 9** Highlight the "thumbprint" property and press **Ctrl-C** to copy it to the clipboard.

**Step 10** If Unity Connection will be configured to use IMAP to access email from an external email server and use calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 9:

**enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"**

If Unity Connection will not be configured to use IMAP but will be configured to use calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 9.

**enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"**

**Step 11** Press **Enter**.

**Step 12** If you want data transmitted as clear text, skip the remaining steps in this procedure and continue with the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 42-4. Otherwise, open the **IIS Manager** application.

**Step 13** Go to **IIS > <server name> > Web Sites > Default Web Site**.

**Step 14** Right-click **Default Web Site** and select **Properties**.

**Step 15** In the **Properties** dialog box, select the **Directory Security** tab.

**Step 16** Under **Secure Communications,** select **Edit**.

**Step 17** Check the **Require Secure Channel** check box.

**Step 18** Select **OK**.

**Step 19** In the **Properties** dialog box, select **OK**.

# Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

### To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **Exchange 2007 External Service Template**.

**Step 4** Confirm that the **Enabled** check box is checked.

**Step 5** In the **Display Name** field, enter a name that will help you identify the service when you configure Unity Connection users to access their email. (For example, in the name of the service, you might include the name of the Exchange server that contains the email that users are accessing.)

**Step 6** In the **Server** field, enter the server name or the fully qualified domain name of one of the Exchange servers that contain emails that you want licensed Unity Connection users to be able to access.

The value that you enter must match the server name or the fully qualified domain name in the certificate for the Exchange server.

**Step 7** In the **Authentication Mode** list, select **NTLM**.

**Step 8** In the **Security Transport Type** list, if you created and installed SSL certificates, select **SSL**. Otherwise, select **None**.

**Step 9** If you selected **SSL** in Step 8, check the **Validate Server Certificates** check box. Otherwise, skip to Step 10.

Self-signed certificates cannot be validated. If you selected **SSL** in Step 8 and you are using self-signed certificates, do not check the **Validate Server Certificates** check box, or Unity Connection will not be able to access Exchange.

**Step 10** Under **Service Capabilities,** check the **User Access to Email in Third-Party Message Store** check box.

**Step 11** Select **Save**.

**Step 12** Repeat Step 2 through Step 13 for each additional Exchange 2007 server that contains emails that you want licensed Unity Connection users to access.

**Step 13** Close Cisco Unity Connection Administration.

# Configuring Users for the External Services in Cisco Unity Connection

Do the following procedure.

**Note** Exchange must have a user for each Unity Connection user that you are configuring.

### To Configure Users for the External Services in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**.

**Step 5** On the **New External Service Accounts** page, in the **External Service** field, select the display name of the applicable external service that you created in the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 42-4.

**Step 6** In the **Email Address** field, enter the email address for the user.

**Step 7** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the User ID setting in Exchange 2007 is the same as the Unity Connection user alias. Unity Connection will sign in the user with the Unity Connection user alias.
- **Use User ID Provided Below**—Enter the User ID setting from Exchange 2007 (useful when the User ID setting is different from the Unity Connection user alias). Unity Connection will sign in the user with the setting in this field.

**Step 8** *(Only when the Use User ID Provided Below option is selected in Step 7)* In the User ID field, enter the User ID setting from Exchange.

**Step 9** In the **Password** field, enter the password from Exchange. Unity Connection will sign in the user with the setting in this field.

**Step 10** Under **Service Capabilities,** check the **User Access to Email in Third-Party Message Store** check box.

**Step 11** Select **Save**.

**Step 12** To check the Exchange configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange, Cisco Unity Connection, and the user.

**Step 13** Repeat Step 2 through Step 12 for all remaining users.

# Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection

If you configure Cisco Unity Connection to integrate with Exchange 2003, users can access emails in an Exchange 2003 message store.

See the following sections:

- Task List for Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection, page 42-7
- Enabling IMAP Access to Exchange in Cisco Unity Connection, page 42-7
- Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only), page 42-8
- Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only), page 42-9
- Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only), page 42-14
- Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only), page 42-14
- Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection, page 42-16
- Configuring Users for the External Services in Cisco Unity Connection, page 42-17

For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 10.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html.

# Task List for Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection

To enable users to emails on an Exchange 2003 message store, complete the following tasks in the order presented.

1. Enable IMAP access to Exchange 2003. See the "Enabling IMAP Access to Exchange in Cisco Unity Connection" section on page 42-7.
2. Create an Active Directory service account that Unity Connection uses to access Exchange data, and grant the account the necessary permissions. See the "Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)" section on page 42-8.
3. Create and install an SSL server certificate on each Exchange server on which you want to access email messages. See the "Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only)" section on page 42-9.
4. *(Optional but recommended)* Configure IIS to refuse unencrypted communications from web clients including Unity Connection. See the "Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only)" section on page 42-14.
5. Configure Unity Connection to trust the SSL certificates that you created and installed on the Exchange servers. See the "Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only)" section on page 42-14.
6. Create Unity Connection external services. See the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 42-16.
7. Configure the users for the external services. See the "Configuring Users for the External Services in Cisco Unity Connection" section on page 42-17.
8. Associate users with a class of service that offers a license to access the TTS feature, and enables them to use it.
9. For each user, create an external service account in Unity Connection that specifies the Exchange server on which the mailbox for the user is stored. This enables the user to access their email when they sign in to Unity Connection by phone.

# Enabling IMAP Access to Exchange in Cisco Unity Connection

Cisco Unity Connection uses the IMAP protocol to access emails in Exchange so the messages can be played by using TTS. By default, Exchange is not configured to allow IMAP access to messages. Do the following procedure to enable IMAP access on each Exchange server that contains emails that you want licensed Unity Connection users to be able to listen to by using TTS.

### To Enable IMAP Access to Exchange in Cisco Unity Connection

**Step 1** On an Exchange server that contains emails that you want licensed Unity Connection users to be able to access, sign in to Windows by using an account that is a member of the local Administrators group.

**Step 2** On the **Windows Start** menu, select **Administrative Tools > Services**.

**Step 3** In the right pane, find the **Microsoft Exchange IMAP4** service.

**Step 4** If the value of the **Status** column is **Started** and the value of the **Startup Type** column is **Automatic**, skip to Step 9.

If the values are different, double-click **Microsoft Exchange IMAP4**.

**Step 5** In the **Microsoft Exchange IMAP4 Properties** dialog box, if **Startup Type** is not Automatic, change it to **Automatic**.

**Step 6** If **Service Status** is not **Started**, select **Start**.

**Step 7** Select **OK** to close the **Microsoft Exchange IMAP4 Properties** dialog box.

**Step 8** Close the Services MMC.

**Step 9** Repeat Step 1 through Step 8 on each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

## Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)

Cisco Unity Connection accesses Exchange 2003 email by using an Active Directory account that acts as a proxy for Unity Connection. Do the following procedure to create the service account and give it the necessary permissions.

### To Create and Configure a Service Account That Can Access Exchange Emails in Cisco Unity Connection

**Step 1** On a computer on which Active Directory Users and Computers and Exchange System Manager are installed, sign in to Windows by using an account that is a member of the Domain Administrators group.

**Step 2** On the Windows Start menu, select **Programs > Microsoft Exchange > Active Directory Users and Computers**.

**Step 3** In the left pane, expand **<Server name>**, right-click **Users**, and select **New > User**.

**Step 4** Follow the on-screen prompts to create a domain user account. Do not create a mailbox.

**Step 5** On the **Windows Start** menu, select **Programs > Microsoft Exchange > System Manager**.

**Step 6** In the left pane, expand **Servers**.

**Step 7** Right-click the name of the Exchange server that contains mailboxes that will be accessed by Cisco Unity Connection, and select **Properties**.

**Step 8** In the <Server name> **Properties** dialog box, select the **Security** tab.

**Step 9** Select **Add**.

**Step 10** In the **Select Users, Computers, or Groups** dialog box, in the **Enter the Object Names to Select** field, enter the name of the service account that you created in Step 4.

**Step 11** Select **Check Names**.

**Step 12** Select **OK** to close the dialog box.

**Step 13** In the <Server name> **Properties** dialog box, in the **Group or User Names** list, select the name of the service account.

**Step 14** In the Permissions For <Account name> list, set the permissions:

a. For **Full Control,** check the **Deny** check box.

**Note** Ensure that the **List Contents and the Read Properties are set to Allow on the Exchange Servers Security** tab.

b. For Receive As, check the **Allow** check box

**Caution** If Exchange server 2003 is configured for Single Inbox, Step 14a. will break Single Inbox permission requirements. Single Inbox needs Receive As, the Send As, and the Administer Information Store permissions to be set to **Allow**.

**Step 15** Select **OK** to close the <Server name> **Properties** dialog box.

**Step 16** Repeat Step 7 through Step 15 for each additional Exchange server on which you want to access emails.

# Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only)

In this section, you create and install an SSL certificate on each Exchange server that contains emails that you want licensed Unity Connection users to be able to access. This prevents Cisco Unity Connection from sending the credentials of the service account that you created in the "Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)" section on page 42-8 over the network as unencrypted text. It also prevents Exchange from sending email content over the network in unencrypted text.

If you use another method to create and install certificates, use the applicable documentation.

This section contains four procedures. Do them in the order listed, as applicable.

If you want to issue SSL certificates by using:

- Microsoft Certificate Services—do the following procedure on any server in the same domain as the Exchange servers that contain emails that you want licensed Unity Connection users to be able to access.
- Another application—see the documentation for that application for installation instructions. Then skip to the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10.
- An external certification authority—skip to the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10.

### To Install the Microsoft Certificate Services Component in Cisco Unity Connection

**Step 1** Locate a Windows Server 2003 disc, which you may be prompted to use to complete the installation of the Microsoft Certificate Services component.

**Step 2** Sign in to Windows by using an account that is a member of the local Administrators group.

**Step 3** On the **Windows Start** menu, select **Settings > Control Panel > Add or Remove Programs**.

**Step 4** In the left pane of the **Add or Remove Programs** control panel, select **Add/Remove Windows Components**.

**Step 5** In the **Windows Components** dialog box, check the **Certificate Services** check box. Do not change any other items.

**Step 6** When the warning appears about not being able to rename the computer or to change domain membership, select **Yes**.

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

**Step 8** On the CA Type page, select **Stand-alone Root CA**, and select **Next**. (A standalone certification authority (CA) is a CA that does not require Active Directory.)

**Step 9** On the **CA Identifying Information** page, in the **Common Name for This CA** field, enter a name for the certification authority.

**Step 10** Accept the default value in the **Distinguished Name Suffix** field.

**Step 11** For **Validity Period,** accept the default value of **5 Years**.

**Step 12** Select **Next**.

**Step 13** On the **Certificate Database Settings** page, select **Next** to accept the default values.

If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, select **Yes** to stop the services.

**Step 14** If you are prompted to insert the Windows Server 2003 disc into the drive, insert either the Cisco Unity Connection disc, which contains the same required software, or a Windows Server 2003 disc.

**Step 15** In the **Completing the Windows Components Wizard** dialog box, select **Finish**.

**Step 16** Close the **Add or Remove Programs** dialog box.

---

Do the following procedure for each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

#### To Create a Certificate Signing Request in Cisco Unity Connection

---

**Step 1** On a server on which Exchange System Manager is installed, sign in to Windows by using an account that is an Exchange Full Administrator.

**Step 2** On the **Windows Start** menu, select **Programs > Microsoft Exchange > System Manager**.

**Step 3** In the left pane, expand **<Organization> > Administrative Groups > <Administrative group> > Servers > <Server name> > Protocols > IMAP4**, where <Administrative group> and <Server name> identify the first Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

**Step 4** Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

**Step 5** In the **Properties** dialog box, select the **Access** tab.

**Step 6** Select **Certificate**.

**Step 7** On the **Welcome to the Web Server Certificate Wizard** page, select **Next**.

**Step 8** On the **Server Certificate** page, select **Create a New Certificate**.

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

**Step 10** On the **Delayed or Immediate Request** page, select **Prepare the Request Now But Send It Later**.

**Step 11** Select **Next**.

**Step 12** On the **Name and Security Settings** page, enter a name for the certificate (for example, <Server name>_Cert).

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

**Step 14** On the Organization Information page, enter the applicable values.

**Step 15** Select **Next**.

**Step 16** On the **Your Site's Common Name** page, enter the computer name of the Exchange server or the fully qualified domain name.

Remember whether you specified the computer name or the fully qualified domain name. You will need this information in a later procedure.

**Caution** The name must exactly match the host portion of any URL that will access the system by using a secure Unity Connection.

**Step 17** Select **Next**.

**Step 18** On the **Geographical Information** page, enter the applicable information.

**Step 19** Select **Next**.

**Step 20** On the **Certificate Request File Name** page, enter a path and filename, and write down the information. You will need it in a later procedure.

If this is not the server on which you installed Microsoft Certificate Services in the "To Install the Microsoft Certificate Services Component in Cisco Unity Connection" procedure on page 42-9, try to select a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.

**Step 21** Select **Next**.

**Step 22** On the **Request File Summary** page, select **Next**.

**Step 23** On the **Completing the Web Server Certificate Wizard** page, select **Finish**.

**Step 24** Select **OK** to close the **Default IMAP4 Virtual Server Properties** dialog box.

**Step 25** Repeat Step 3 through Step 24 to create a certificate signing request for each additional Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

**Step 26** Close **Exchange System Manager.**

**Step 27** If Microsoft Certificate Services is on another server and you were not able to save the certificate request files in a network location accessible to that server, copy the certificate request files to a removable medium (diskette, CD, or DVD).

**Step 28** If you are not using an external certification authority, you are finished with this procedure.

If you are using an external certification authority, send the certificate request file that you specified in Step 20 to the CA. When the certificate returns from the CA, skip to the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 42-13.

Issue certificates or have them issued for each of the certificate signing requests that you created in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10:

- If you are using Microsoft Certificate Services to issue certificates, do the following procedure.
- If you are using an application other than Microsoft Certificate Services, see the documentation for the application for information on issuing server certificates and exporting a trust certificate. When you export the trust certificate, which is uploaded to the Cisco Unity Connection server later in this chapter, export it in base-64 encoded X.509 format with a .pem filename extension. Then continue with the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 42-13.
- If you are using an external certification authority (CA) to issue certificates, send the certificate signing requests to the CA. Request that the CA provide the trust certificate, which is uploaded to the Cisco Unity Connection server later in this chapter, in base-64 encoded X.509 format with a .pem filename extension. When the certificates are returned, continue with the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 42-13.

### To Issue the Server Certificate in Cisco Unity Connection (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

**Step 1** On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the Domain Admins group.

**Step 2** On the **Windows Start** menu, select **Programs > Administrative Tools > Certification Authority**.

**Step 3** In the left pane, expand **Certification Authority (Local) > <Certification authority name>**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the "To Install the Microsoft Certificate Services Component in Cisco Unity Connection" procedure on page 42-9.

**Step 4** Right-click the name of the certification authority, and select **All Tasks > Submit New Request**.

**Step 5** In the **Open Request File** dialog box, browse to the location of the first certificate signing request file that you created in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10, and double-click the file.

**Step 6** In the left pane of **Certification Authority,** select **Pending Requests**.

**Step 7** Right-click on the pending request that you submitted in Step 5, and select **All Tasks > Issue**.

**Step 8** In the left pane of **Certification Authority**, select **Issued Certificates**.

**Step 9** Right-click the new certificate, and select **All Tasks > Export Binary Data**.

**Step 10** In the **Export Binary Data** dialog box, in the **Columns that Contain Binary Data** list, select **Binary Certificate**.

**Step 11** Select **Save Binary Data to a File**.

**Step 12** Select **OK**.

**Step 13** In the **Save Binary Data** dialog box, enter a path and filename, and write down the information. You will need it in a later procedure.

If this is not a server on which Exchange System Manager is installed, try to select a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.

**Step 14** Select **OK**.

**Step 15** If you created more than one certificate signing request in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10, repeat Step 9 through Step 11 for each certificate signing request listed under Issued Certificates.

**Step 16** Close **Certification Authority.**

**Step 17** If Exchange System Manager is on another server, and if you were not able to save the certificate request files in a network location accessible to that server, copy the certificate request files to a removable medium (diskette, CD, or DVD).

---

Do the following procedure for each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

#### To Install the Server Certificate in Cisco Unity Connection

---

**Step 1** On a computer on which Exchange System Manager is installed, sign in to Windows by using an account that is an Exchange Full Administrator.

**Step 2** On the **Windows Start** menu, select **Programs > Microsoft Exchange > System Manager**.

**Step 3** In the left pane, expand **<Organization name> > Administrative Groups > <Administrative group> > Servers > <Server name> > Protocols > IMAP4**, where <Administrative group> and <Server name> identify the first Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

**Step 4** Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

**Step 5** Select the **Access** tab.

**Step 6** Select **Certificate**.

**Step 7** On the **Welcome to the Web Server Certificate Wizard,** select **Next**.

**Step 8** On the **Pending Certificate Request** page, select **Process the Pending Request and Install the Certificate**.

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

**Step 10** On the **Process a Pending Request** page, browse to the location where you saved the certificates, and specify the server certificate that you created using Microsoft Certificate Services or another application, or that you got from an external CA.

You may have to change the value of the **Files of Type list to All Files (*.*)** to see the certificates.

**Step 11** Select **Next**.

**Step 12** On the **Certificate Summary** page, select **Next**.

**Step 13** On the **Completing the Web Server Certificate Wizard** page, select **Finish**.

**Step 14** Close the **Default IMAP4 Virtual Server Properties** dialog box.

**Step 15** Repeat Step 3 through Step 14 for each certificate that you want to install.

**Step 16** Close **Exchange System Manager.**

---

# Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only)

Earlier in this chapter, you enabled IMAP access to Exchange, and you secured the IMAP connections between the Cisco Unity Connection server and one or more Exchange servers. To prevent Exchange from allowing access through unsecured IMAP connections, do the following procedure on each Exchange server that you are allowing Cisco Unity Connection to access.

### To Configure Exchange to Require Secure Communication with Cisco Unity Connection (Optional But Recommended)

**Step 1** On an Exchange server that contains emails that you want licensed Unity Connection users to be able to access, sign in to Windows by using an account that is an Exchange Full Administrator.

**Step 2** On the **Windows Start** menu, select **Programs > Microsoft Exchange > System Manager**.

**Step 3** In the left pane, expand **Servers > <Server name> > Protocols > IMAP4 > Default IMAP4 Virtual Server**.

**Step 4** Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

**Step 5** Select the **Access** tab.

**Step 6** Select **Communication**.

**Step 7** Select **Require Secure Channel**.

**Step 8** Select **OK**.

**Step 9** Close the Properties dialog box.

**Step 10** In the left pane, for the same server, expand **Servers > <Server name> > Protocols > IMAP4 > Default IMAP4 Virtual Server**.

**Step 11** In the **System Manager** toolbar, select the **Stop** icon.

**Step 12** Wait a few seconds.

**Step 13** Select the **Play** icon.

**Step 14** Repeat Step 1 through Step 13 for each additional Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

# Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only)

To make the Cisco Unity Connection server trust the certificates for the Exchange servers, you need to upload, to the root certificate store on the Unity Connection server, a trust certificate for each certification authority that issued certificates. Typically, you will use the same certification authority (for example, Microsoft Certificate Services or VeriSign) to issue all certificates.

### To Configure the Cisco Unity Connection Server to Trust Exchange Certificates

**Step 1** If you used Microsoft Certificate Services to issue the certificates, continue with Step 2.

If you used another application or an external certification authority to issue the certificates, skip to Step 21 to upload the trust certificates, in base-64-encoded X.509 format, to the root certificate store on the Unity Connection server.

**Step 2** On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the local Administrators group.

**Step 3** On the **Windows Start** menu, select **Programs > Administrative Tools > Certification Authority**.

**Step 4** In the left pane, expand **Certification Authority (Local)**.

**Step 5** Right-click the name of the certification authority, and select **Properties**.

**Step 6** In the <Certification authority name> **Properties** dialog box, on the **General** tab, in the CA Certificates list, select the name of one of the certificates that you issued for the Exchange servers.

**Step 7** Select **View Certificate.**

**Step 8** In the Certificate dialog box, select the **Details** tab.

**Step 9** Select **Copy to File**.

**Step 10** On the **Welcome to the Certificate Export Wizard** page, select **Next**.

**Step 11** On the **Export File Format** page, select **Base-64 Encoded X.509 (.CER)**.

**Step 12** Select **Next**.

**Step 13** On the **File to Export** page, enter a temporary path and filename for the trust certificate (for example, c:\cacert.pem). Use the filename extension **.pem**.

**Caution** The trust certificate must have a .pem filename extension or you will not be able to upload it on the Unity Connection server.

**Step 14** Write down the path and filename because you will need it later in this procedure.

**Step 15** Select **Next**.

**Step 16** On the **Completing the Certificate Export Wizard** page, select **Finish**.

**Step 17** Select **OK** to close the “Export successful” message box.

**Step 18** Select **OK** to close the Certificate dialog box.

**Step 19** Select **OK** to close the <Server name> Properties dialog box.

**Step 20** Close **Certification Authority**.

**Step 21** Copy the trust certificate to a network location that is accessible to the Unity Connection server.

**Step 22** On the Unity Connection server, sign in to Cisco Unified Operating System Administration.

**Step 23** On the **Security** menu, select **Certificate Management**.

**Step 24** On the **Certificate List** page, select **Upload Certificate**.

**Step 25** On the **Upload Certificate** page, in the Certificate Name list, select **Unity Connection-trust**.

**Step 26** In the **Root Certificate** field, enter the name of the certificate file that you issued using Microsoft Certificate Services or another certification authority, or that you got from a CA.

**Step 27** Select **Browse**.

**Step 28** In the **Choose File** dialog box, browse to the location of the certificate file, select the name of the file, and select **Open**.

**Step 29** On the **Upload Certificate** page, select **Upload File**.

**Step 30** When the Status area reports that the upload succeeded, select **Close**.

**Step 31** If you issued certificates or had them issued by more than one certification authority, repeat Step 24 through Step 30 for each trust certificate.

# Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

### To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

**Step 2** On the **Search External Services** page, select **Add New**.

**Step 3** On the **New External Service** page, in the **Type** list, select **Exchange 2003 External Service Template**.

**Step 4** Confirm that the **Enabled** check box is checked.

**Step 5** In the **Display Name** field, enter a name that will help you identify the service when you configure Unity Connection users to access their email. (For example, in the name of the service, you might include the name of the Exchange server that contains the email that users are accessing.)

**Step 6** In the **Server** field, enter the server name or the fully qualified domain name of one of the Exchange servers that contain emails that you want licensed Unity Connection users to be able to access.

The value that you enter must match the server name or the fully qualified domain name in the certificate for the Exchange server, which you specified in Step 16 of the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 42-10.

**Step 7** In the **Authentication Mode** list, select **NTLM**.

**Step 8** In the **Security Transport Type** list, if you created and installed SSL certificates, select **SSL**. Otherwise, select **None**.

**Step 9** If you selected SSL in Step 8, check the **Validate Server Certificates** check box. Otherwise, continue to Step 10.

Self-signed certificates cannot be validated. If you selected **SSL** in Step 8 and you are using self-signed certificates, do not check the **Validate Server Certificates** check box, or Unity Connection will not be able to access Exchange.

**Step 10** Under **Service Credentials,** in the **Alias** field, enter the Active Directory user sign-in name of the service account that you created in the "To Create and Configure a Service Account That Can Access Exchange Emails in Cisco Unity Connection" procedure on page 42-8. Use the format **<Domain name>\<Account name>**.

**Step 11** In the **Password** field, enter the password for the service account.

**Step 12** Under **Service Capabilities,** check the **User Access to Email in Third-Party Message Store** check box.

**Step 13** Select **Save**.

**Step 14** Repeat Step 2 through Step 13 for each additional Exchange server that contains emails that you want licensed Unity Connection users to be able to access.

**Step 15** Close Cisco Unity Connection Administration.

# Configuring Users for the External Services in Cisco Unity Connection

Do the following procedure.

**Note** Exchange must have a user for each Unity Connection user that you are configuring.

### To Configure Users for the External Services in Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

**Step 2** On the **Search Users** page, select the alias of a user.

**Step 3** On the **Edit User Basics** page, on the **Edit** menu, select **External Service Accounts**.

**Step 4** On the **External Service Accounts** page, select **Add New**.

**Step 5** On the **New External Service Accounts** page, in the **External Service** field, select the display name of the applicable external service that you created in the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 42-16.

**Step 6** In the **Email Address** field, enter the email address for the user.

**Step 7** In the **Sign-In Type** field, select the applicable option:

- **Use Unity Connection Alias**—This option is useful when the User ID setting in Exchange 2003 is the same as the Unity Connection user alias. Unity Connection will sign in the user with the Unity Connection user alias.
- **Use User ID Provided Below**—Enter the User ID setting from Exchange 2003 (useful when the User ID setting is different from the Unity Connection user alias). Unity Connection will sign in the user with the setting in this field.

**Step 8** *(Only when the Use User ID Provided Below option is selected in Step 7)* In the **User ID** field, enter the User ID setting from Exchange.

**Step 9** Under **Service Capabilities,** check the **User Access to Email in Third-Party Message Store** check box.

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

**Step 11** To check the Exchange configuration for the user, select **Test**. The **Task Execution Results** window appears with the test results.

If any part of the test fails, verify the configuration for Exchange, Cisco Unity Connection, and the user.

**Step 12** Repeat Step 2 through Step 11 for all remaining users.

# Reports in Cisco Unity Connection 10.x

You can use Cisco Unity Connection reports to gather information about system configuration and call handlers. See the following sections:


- Reports Overview in Cisco Unity Connection 10.x, page 43-1
- Setting Report Configuration Parameters in Cisco Unity Connection 10.x, page 43-4
- Generating and Viewing Reports in Cisco Unity Connection 10.x, page 43-5


## Reports Overview in Cisco Unity Connection 10.x

You can generate the following reports in Cisco Unity Connection Serviceability:

*Table 43-1 Reports Available in Cisco Unity Connection*

| Report Name | Description of Output |
|---|---|
| Phone Interface Failed Sign-In | Includes the following information for every failed attempt to sign in to Cisco Unity Connection by phone:<br>• Username, alias, caller ID, and extension of user who failed to sign in.<br>• Date and time the failed sign-in occurred.<br>• Whether the maximum number of failed sign-ins has been reached for the user. |
| Users | Includes the following information for each user:<br>• Last name, first name, and alias.<br>• Information that identifies the Unity Connection or Cisco Unified CMBE server associated with the user.<br>• Billing ID, class of service, and extension.<br>• Whether the account is locked.<br>• Whether the user has enabled personal call transfer rules. |

*Table 43-1 Reports Available in Cisco Unity Connection (continued)*

| Report Name | Description of Output |
|---|---|
| Message Traffic | Includes totals for the following traffic categories:<br>• Voice.<br>• Fax.<br>• Email.<br>• Non-delivery receipt (NDR).<br>• Delivery receipt.<br>• Read receipt.<br>• Hourly totals.<br>• Daily totals. |
| Port Activity | Includes the following information for voice messaging ports:<br>• Name.<br>• Number of inbound calls handled.<br>• Number of outbound MWI calls handled.<br>• Number of outbound AMIS calls handled.<br>• Number of outbound notification calls handled.<br>• Number of outbound TRAP calls handled.<br>• Total number of calls handled. |
| Mailbox Store | Includes the following information about the specified mailbox stores:<br>• Mail database name.<br>• Display name.<br>• Server name.<br>• Whether access is enabled.<br>• Mailbox store size.<br>• Last error.<br>• Status.<br>• Whether the mail database can be deleted. |
| Dial Plan | Includes a list of the search spaces configured on the Unity Connection or Cisco Unified CMBE server, with an ordered list of partitions assigned to each search space.<br>If the server is part of a Digital Network, also lists the search spaces and associated partition membership on every other Unity Connection location on the network. |
| Dial Search Scope | Includes a list of all users and their extensions in the specified partition that is configured in the Unity Connection directory. If a partition is not specified, lists all users and their extensions for all partitions that are configured in the directory. |

*Table 43-1 Reports Available in Cisco Unity Connection (continued)*

| Report Name | Description of Output |
|---|---|
| User Phone Sign-In and MWI | Includes the following information about phone sign-ins, MWI activity, and message notifications to phone devices per user:<br>• Name, extension, and class of service.<br>• Date and time for each activity.<br>• The source of each activity.<br>• Action completed (for example, Sign-in, MWI On or Off, and Phone Dialout).<br>• Dial out number and results (applicable only for message notifications to phone devices).<br>• The number of new messages for a user at time of sign-in. |
| User Message Activity | Includes the following information about messages sent and received, per user:<br>• Name, extension, and class of service.<br>• Date and time for each message.<br>• Type of message.<br>• Action completed (for example, new message, message saved, and so on).<br>• Information on the message sender. |
| Distribution Lists | Includes the following information:<br>• Name and display name of the list.<br>• Date and time the list was created. (Date and time are given in Greenwich Mean Time.)<br>• A count of the number of users included in the list.<br>• If the Include List Members check box is checked, a listing of the alias of each user who is a member of the list. |
| User Lockout | Includes user alias, the number of failed sign-in attempts for the user, credential type (a result of “4” indicates a sign-in attempt from the Unity Connection conversation; a result of “3” indicates a sign-in attempt from a web application), and the date and time that the account was locked.<br>(Date and time are given in Greenwich Mean Time.) |
| Unused Voice Mail Accounts | Includes user alias and display name, and the date and time that the user account was created.<br>(Date and time are given in Greenwich Mean Time.) |
| Transfer Call Billing | Includes the following information for each call:<br>• Name, extension, and billing ID of the user.<br>• Date and time that the call occurred.<br>• The phone number dialed.<br>• The result of the transfer (connected, ring-no-answer (RNA), busy, or unknown). |

*Table 43-1 Reports Available in Cisco Unity Connection (continued)*

| Report Name | Description of Output |
|---|---|
| Outcall Billing Detail | Includes the following information, arranged by day and by the extension of the user who placed the call:<br>• Name, extension, and billing ID.<br>• Date and time the call was placed.<br>• The phone number called.<br>• The result of the call (connected, ring-no-answer (RNA), busy, or unknown).<br>• The duration of the call in seconds. |
| Outcall Billing Summary | Arranged by date and according to the name, extension, and billing ID of the user who placed the call, and is a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span. |
| Call Handler Traffic | Includes the following information for each call handler, in rows for each hour of a day:<br>• Total number of calls.<br>• Number of times each key on the phone keypad was pressed.<br>• Extension.<br>• Invalid extension.<br>• Number of times the after greeting action occurred.<br>• Number of times the caller hung up. |
| System Configuration | Includes detailed information about all aspects of the configuration of the Unity Connection system. |
| SpeechView Activity Report by User | Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user. |
| SpeechView Activity Summary Report | Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. When messages are sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once. |

# Setting Report Configuration Parameters in Cisco Unity Connection 10.x

Cisco Unity Connection is automatically set to gather and store data from which you can generate reports. The following parameters can be adjusted, depending on the report output that you want to generate. All report parameter settings are found on the System Settings > Advanced > Reports page in Cisco Unity Connection Administration.

- **Milliseconds Between Data Collection Cycles**—Set by default to 30 minutes (1,800,000 milliseconds). This setting controls the amount of time Unity Connection waits between cycles of gathering report data.

- **Days to Keep Data in Reports Database**—Set by default to 90 days. Note that even if you specify more than this number of days in the time range for the report you are generating, the number of days of data is limited by what you set here.
- **Maximum Records in Report Output**—Set by default to 25,000 records. The maximum value allowed for this field is 30,000 records. If the report you want to generate exceeds the maximum number of records allowed, you can generate the report in pieces, for example by reducing the date range or number of user accounts included in each iteration.

**Note** The Maximum Records in Report Output setting for the User Message Activity Report has been restricted to 15,000 records—rather than the default of 25,000 records—because of the size of the report.

- **Minimum Records Needed to Display Progress Indicator**—Set by default to 2,500 records. The maximum value allowed for this field is 10,000 records. The purpose of the progress indicator is to warn you if the report you request is large and likely to take a long time to complete. In Unity Connection, reports are generated from within a browser, and the browser session must be kept open while the report is being generated. Depending on the size of the database, and the type of report being generated, a report can take a long time to generate; meanwhile, you are unable to use the browser, and must keep the Connection Administration session open.

## Archiving Report Data

Reports data is gradually written over, depending on parameters that you set for retention of data. We recommend that if you want to keep reports for historical purposes, you develop a schedule for regularly generating reports, and save them in a location separate from the Cisco Unity Connection server.

# Generating and Viewing Reports in Cisco Unity Connection 10.x

You can generate and view reports in Cisco Unity Connection Serviceability. To go to Cisco Unity Connection Serviceability, in the navigation box in the upper-right corner of Cisco Unity Connection Administration, select Cisco Unity Connection Serviceability and select Go.

For details on generating and viewing reports for Cisco Unity Connection Serviceability, see the *Administration Guide for Cisco Unity Connection Serviceability* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

# Integrating Cisco Unity Connection 10.x with an LDAP Directory

If you are using a supported LDAP-compliant directory as your corporate directory and if you do not want to separately maintain basic user information in Cisco Unity Connection, you can:

- Create Unity Connection users by importing user data from the LDAP directory, and
- Configure Unity Connection to periodically resynchronize Unity Connection data with data in the LDAP directory.

For a list of the LDAP directories that are supported for use with Unity Connection, see the "Requirements for an LDAP Directory Integration" section in *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.

See the following sections:


- Integrating Cisco Unified Communications Manager and Cisco Unity Connection 10.x with an LDAP Directory, page 44-2
- Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 10.x Users with LDAP Users, page 44-2
- Activating the Cisco DirSync Service in Cisco Unity Connection 10.x, page 44-4
- Enabling LDAP Synchronization in Cisco Unity Connection 10.x, page 44-4
- Disabling LDAP Synchronization in Cisco Unity Connection 10.x, page 44-5
- Converting Phone Numbers into Extensions, page 44-5
- Converting Phone Numbers into Extensions, page 44-5
- Uploading SSL Certificates on the Cisco Unity Connection 10.x Server, page 44-7
- Configuring LDAP Authentication in Cisco Unity Connection 10.x, page 44-8
- Disabling LDAP Authentication, page 44-9
- Selecting the LDAP Users to Import into Cisco Unity Connection 10.x, page 44-10
- Filtering LDAP Users in Cisco Unity Connection 10.x, page 44-12
- Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x, page 44-14
- Changing LDAP Directory Configurations in Cisco Unity Connection 10.x, page 44-15
- Deleting LDAP Directory Configurations in Cisco Unity Connection 10.x, page 44-16
- Changing Which LDAP Field Is Mapped to the Alias Field in Unity Connection, page 44-16

# Integrating Cisco Unified Communications Manager and Cisco Unity Connection 10.x with an LDAP Directory

If Unity Connection is integrated with a Cisco Unified CM phone system, and if you want to integrate both Unity Connection and Cisco Unified CM with an LDAP directory, you must separately integrate each application with the LDAP directory. Integrating only one of the applications with an LDAP directory is not sufficient to allow the other application to synchronize or authenticate with the LDAP directory.

For information on integrating Cisco Unified CM with an LDAP directory, start with the "LDAP System Configuration" chapter in the "System Configuration" section of the applicable *Cisco Unified Communications Manager Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

For information on integrating Unity Connection with an LDAP directory, start with the "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 10.x Users with LDAP Users" section on page 44-2.

# Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 10.x Users with LDAP Users

To configure LDAP and to create users by importing user data from the LDAP directory, do the following tasks:

1. Turn on the Cisco DirSync service. See the "Activating the Cisco DirSync Service in Cisco Unity Connection 10.x" section on page 44-4.
2. Enable LDAP synchronization. See the "Enabling LDAP Synchronization in Cisco Unity Connection 10.x" section on page 44-4.

   If you are using LDAP authentication to authenticate user access to Unity Connection web applications or IMAP access to Unity Connection voice messages, you must enable LDAP synchronization.
3. *(Optional)* If the phone numbers stored in the LDAP directory are not in the same format as the extensions that you want to use in Unity Connection, specify a filter that converts phone numbers into extensions when you import LDAP data into Unity Connection. See the applicable section:
   - Converting Phone Numbers into Extensions, page 44-5
   - Converting Phone Numbers into Extensions, page 44-5

   If you use the Bulk Administration Tool (BAT) to create users, you may be able to achieve the same or better results than you could by specifying a filter in this step. In Task 9., if you use BAT, you export user data to a CSV file, edit the CSV file, and import the edited file. During this process, you can open the CSV file in a spreadsheet application and possibly create a formula that is more effective than the regular expression that you can specify for the filter discussed in the "Converting Phone Numbers into Extensions" section on page 44-5.

4. *(Optional)* If you want to use SSL to encrypt the usernames and passwords that are sent to the LDAP server for authentication and/or you want to use SSL to encrypt the data that is passed from the LDAP server to the Unity Connection server during synchronization, export an SSL certificate from the applicable LDAP servers and upload the certificates on all Unity Connection servers. See the "Uploading SSL Certificates on the Cisco Unity Connection 10.x Server" section on page 44-7.
5. *(Optional)* If you want Unity Connection users who access a Unity Connection web application or who access Unity Connection voice messages by using an IMAP email application to authenticate their username and password against the LDAP directory, configure LDAP authentication. See the "Configuring LDAP Authentication in Cisco Unity Connection 10.x" section on page 44-8.
6. Select the user search bases that you will specify when you create LDAP directory configurations in Task 8. See the "Selecting the LDAP Users to Import into Cisco Unity Connection 10.x" section on page 44-10.
7. *(Required if the number of users in all user search bases is greater than 60,000, optional otherwise)* If the user search bases that you selected in Task 6. do not give you enough control over which LDAP users are synchronized with Unity Connection users, you may want to specify one or more LDAP filters. See the "Filtering LDAP Users in Cisco Unity Connection 10.x" section on page 44-12.
8. Add one or more LDAP directory configurations, which define the LDAP directory and user search bases in which Unity Connection accesses data, and import data from the LDAP directory into a hidden Cisco Unified CM database on the Unity Connection server. When you create Unity Connection users that are linked to LDAP users or you convert existing Unity Connection users to users who are integrated with an LDAP directory, the data on the LDAP users is taken from the Cisco Unified CM database on the Unity Connection server. See the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x" section on page 44-14.
9. If you are synchronizing existing Unity Connection users with users in an LDAP directory, see the applicable section in the "Creating User Accounts from LDAP User Data or Changing LDAP Integration Status for Existing Users in Cisco Unity Connection 10.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/0xcucmacx.html.
   - See the "Changing the LDAP Integration Status of Unity Connection Users " section.
   - See the "Integrating Existing Cisco Unity Connection User Accounts with LDAP User Accounts" section.

   If you are creating new Unity Connection users who are synchronized with users in an LDAP directory, use one of the following methods:

   - If you are creating a small number of users (a few hundred or fewer) and if you were able to create a regular expression to convert LDAP phone numbers into Unity Connection extensions, you can use the Import Users tool.
   - If you are creating a larger number of users or if you were not able to create a regular expression to convert LDAP phone numbers into Unity Connection extensions, export user data to a CSV file by using the Bulk Administration Tool, reformat the data by using a spreadsheet application (if necessary), and import the data by using the Bulk Administration tool.

# Activating the Cisco DirSync Service in Cisco Unity Connection 10.x

The Cisco DirSync service must be turned on for Unity Connection to access an LDAP directory. Do the following procedure.

### To Turn On the Cisco DirSync Service

**Step 1** Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

**Step 2** On the **Tools** menu, select **Service Activation**.

**Step 3** Under **Directory Services,** check the **Cisco DirSync Service** check box.

**Step 4** Select **Save**, and select **OK** to confirm.

# Enabling LDAP Synchronization in Cisco Unity Connection 10.x

LDAP synchronization must be enabled for Unity Connection to access an LDAP directory. Do the following procedure.

### To Enable LDAP Synchronization

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

**Step 2** Expand **System Settings > LDAP**, then select **LDAP Setup**.

**Step 3** On the **LDAP Setup** page, check the **Enable Synchronizing from LDAP Server** check box.

**Step 4** In the **LDAP Server Type** list, select the type of LDAP server that you want to access.

When you are configuring Unity Connection for Microsoft Active Directory 2008 Lightweight Directory Services, select **Microsoft Active Directory Application Mode**.

**Step 5** In the **LDAP Attribute for User ID** list, select the field in the LDAP directory whose data you want to appear in the Alias field in Unity Connection. Note the following requirements:

- The field that you select must have a value for every user in the LDAP directory.
- Every value for that field must be unique.

**Caution** If you select a field other than sAMAccountName, when users sign in to the Cisco PCA or an IMAP client or sign in to the Web Inbox, they must enter their Unity Connection alias and their LDAP password.

**Caution** If you later need to change the field that you select now, and if you have already created LDAP directory configurations on the LDAP Directory page, you must delete all LDAP directory configurations, change the value here, and recreate all LDAP directory configurations. For more information, see the "Changing Which LDAP Field Is Mapped to the Alias Field in Unity Connection" section on page 44-16.

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

# Disabling LDAP Synchronization in Cisco Unity Connection 10.x

If you want to temporarily disable LDAP synchronization, do the following procedure.

### To Disable LDAP Synchronization

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

**Step 2** Expand **System Settings > LDAP**, then select **LDAP Setup**.

**Step 3** On the **LDAP Setup** page, uncheck the **Enable Synchronizing from LDAP Server** check box.

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

# Converting Phone Numbers into Extensions

If you want to map phone numbers in the LDAP directory to extensions in Unity Connection but the phone numbers do not match the extensions, you can add a regular expression and a replacement pattern that together convert the phone numbers into extensions:

- The regular expression determines which phone numbers to operate on (for example, phone numbers that are 10 digits long) and the portion of the phone numbers to use as a basis for the extensions (for example, the last four digits).
- The replacement pattern specifies either to use the values selected by the regular expression or to perform additional operations (for example, prepend an 8).

Unity Connection uses the regular expression package of the Java library. Table 44-1 lists some examples of the conversions that are possible with the expanded functionality. For more information, refer to a reference on regular expressions; several are available in print and online; do a web search on "regular expression."

Note the following:

- Unity Connection automatically removes non-numeric characters from the phone number, so the regular expression does not need to account for non-numeric characters.
- If a phone number in the LDAP directory does not match the regular expression, the corresponding Unity Connection Extension field will contain the numeric portion of the LDAP phone number. For example, if a phone number begins with 425 and the regular expression gets the last four digits of the LDAP phone number as the Unity Connection extension, but only if the LDAP phone number starts with 206, the Extension field for that Unity Connection user will contain the entire LDAP phone number minus any non-numeric characters.
- LDAP phone numbers are converted to Unity Connection extensions only once, when you first synchronize Unity Connection data with LDAP data. On subsequent, scheduled synchronizations, values in the Unity Connection Extension field are not updated with changes to the LDAP phone number. As a result, you can change the LDAP phone number as required, including specifying a completely different number, and the extension will not be overwritten the next time that Unity Connection synchronizes data with the LDAP directory.

- You can often write more than one combination of regular expression and replacement pattern that produces the same result.

***Table 44-1 Example Phone Number Conversions for Unity Connection***

| Example Conversion Operation | Regular Expression for LDAP Phone Number Pattern | Replacement Pattern |
|---|---|---|
| Use the LDAP phone number as the Unity Connection extension. | (.*) | $1 |
| Use the last four digits of the LDAP phone number as the Unity Connection extension. | .*(\d{4}) | $1 |
| Use the first four digits of the LDAP phone number as the Unity Connection extension. | (\d{4}).* | $1 |
| Append a 9 to the left of the last four digits of the LDAP phone number. | .*(\d{4}) | 9$1 |
| Embed the digits 555 between the first three digits and the last four digits of the LDAP phone number. | (\d{3}).*(\d{4}) | $1555$2 |
| Use the last four digits of the LDAP phone number as the Unity Connection extension, but only if the LDAP phone number is between seven and ten digits long. | \d{3,6}(\d{4}) | $1 |
| Use the last four digits of the LDAP phone number as the Unity Connection extension, but only if the LDAP phone number starts with 206. | 206.*(\d{4}) | $1 |
| Prepend 85 to the left of the rightmost 5 digits of the LDAP phone number, but only if the LDAP phone number is 10-digit long. | \d{5}(\d{5}) | 85$1 |
| Remove the leftmost three digits of the LDAP phone number but only if the LDAP phone number is 13 digits long and the first three digits are 011. | 011(\d{10}) | $1 |
| Remove the leftmost six digits of the LDAP phone number and then prepend 52 to the remaining digits, but only if the LDAP phone number is 10 digits long and the first three digits are 206. | 206\d{3}(\d{4}) | 52$1 |

If the expanded support for regular expressions cannot convert phone numbers in your LDAP directory into Unity Connection extensions, you may want to explore whether a formula in a spreadsheet application is able to produce the results that you want. If so, when you create new Unity Connection users from LDAP data or synchronize existing Unity Connection users with LDAP users, you can manipulate phone number data in the CSV file using a spreadsheet application before you import the data back into Unity Connection. See either the “Creating Cisco Unity Connection 10.x Users from LDAP Data by Using the Bulk Administration Tool” section or the ““Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool ” section, as applicable, in the “Creating User Accounts from LDAP User Data or Changing LDAP Integration Status for Existing Users in Cisco Unity Connection 10.x” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

### To Add a Regular Expression and Replacement Pattern That Convert LDAP Phone Numbers into Cisco Unity Connection Extensions

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then select **Phone Number Conversion**.

**Step 2** In the **Regular Expression for LDAP Phone Number Pattern** field, enter a regular expression that identifies:

- Which phone numbers in the LDAP directory you want to convert to extensions (for example, 10-digit phone numbers that begin with 206).
- The portion of the phone numbers to use as a basis for the extensions (for example, the last four digits).

**Step 3** In the **Replacement Pattern** field, enter a value that specifies either to use the values selected by the regular expression or to perform additional operations (for example, prepend an 8).

**Caution** Unity Connection validates the syntax of the regular expression but does not validate the replacement pattern, and also cannot validate the result of the regular expression and the replacement pattern. We recommend that you verify the results on the Import Users page of Connection Administration before you create Unity Connection subscribers.

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

# Uploading SSL Certificates on the Cisco Unity Connection 10.x Server

If you want to use SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server, do the following procedure.

**Note** You must also specify servers by host name instead of by IP address, and check the "Use SSL" check box for each LDAP server that you configure for synchronization (see the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x" section on page 44-14), or for authentication (see the "Configuring LDAP Authentication in Cisco Unity Connection 10.x" section on page 44-8).

### To Upload SSL Certificates from the LDAP Directory Servers

**Step 1** Export the SSL certificate from the LDAP server with which you want Unity Connection to synchronize data and from the LDAP server that you want Unity Connection to access when authenticating user sign-ins, if any.

If you want to configure redundant LDAP servers for synchronization and/or for authentication, export an SSL certificate from each LDAP server with which you want Unity Connection to synchronize or authenticate.

**Step 2** On the Unity Connection server, sign in to Cisco Unified Operating System Administration.

**Step 3** On the **Security** menu, select **Certificate Management**.

**Step 4** Upload the directory certificate trust that you exported in Step 1:

- Upload the directory certificate trust to tomcat-trust.

If you want this Unity Connection server to synchronize with more than one LDAP server or to authenticate with more than one LDAP server, upload the directory certificate trusts from all of the LDAP servers.

For more information on uploading directory certificate trusts and on restarting the Cisco Dirsync and Cisco Tomcat services, on the Help menu, select **This Page**.

**Caution** You must restart the Cisco DirSync and Cisco Tomcat services, or LDAP synchronization and authentication will fail.

**Step 5** If you are configuring Unity Connection clustering, or if you are configuring a Digital Network, repeat Step 2 through Step 4 on the other Unity Connection servers.

# Configuring LDAP Authentication in Cisco Unity Connection 10.x

Some companies want the convenience of single sign-on credentials for their applications. To authenticate sign-ins to Unity Connection web applications against user credentials in an LDAP directory, you must synchronize Unity Connection user data with user data in the LDAP directory as described in the "LDAP Synchronization" section in *Design Guide for Cisco Unity Connection*.

Only passwords for Unity Connection web applications (Cisco Unity Connection Administration for administration, Cisco Personal Communications Assistant for end users), and for IMAP email applications that are used to access Unity Connection voice messages, are authenticated against the corporate directory. You manage these passwords by using the administration application for the LDAP directory. When authentication is enabled, the password field is no longer displayed in Cisco Unity Connection Administration.

For telephone user interface or voice user interface access to Unity Connection voice messages, numeric passwords (PINs) are still authenticated against the Unity Connection database. You manage these passwords in Connection Administration; users manage PINs by using the phone interface or the Messaging Assistant web tool.

The LDAP directories that are supported for LDAP authentication are the same as those supported for synchronization. See the "Requirements for an LDAP Directory Integration" section in the *System Requirements for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/0xcucsysreqs.html.

If you want to use LDAP usernames and passwords to authenticate sign-ins to Cisco Unity Connection web applications or IMAP access to Unity Connection voice messages, do the following procedure to configure LDAP authentication.

**Note** You cannot use LDAP usernames and passwords to authenticate sign-ins for the administrator account that you created during installation. The administrator account is used to sign on to Cisco Unified Operating System Administration, the Disaster Recovery System, and the command line interface.

**To Configure LDAP Authentication**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, and select **LDAP Authentication**.

**Step 2** Check the Use LDAP Authentication for **End Users** check box.

**Step 3** Enter other values as applicable. For more information, on the **Help** menu, select **This Page**.

If you change the value of the Host Name or IP Address for Server field, and if IMAP clients are accessing Unity Connection, restart the Unity Connection IMAP Server service. If other web applications are accessing Unity Connection (for example, Cisco Personal Communications Assistant), restart the server.

If you uploaded SSL certificates to the Unity Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 44-7:

- Check the **Use SSL** check box for every LDAP server that you specify in the Host Name or IP Address for Server field.
- In the **Host Name or IP Address for Server** field, specify the host name of the server, or authentication will probably fail for IMAP clients. If you specify an IP address and the SSL certificate identifies the LDAP server only by host name (which is common—certificates rarely include the IP address of a server), Unity Connection cannot verify the identity of the LDAP server.

**Note** With some supported LDAP directories, you cannot specify redundant LDAP servers. For information on the LDAP directories with which Unity Connection allows you to specify redundant servers, see the "Requirements for an LDAP Directory Integration" section in *System Requirements for Cisco Unity Connection Release 10.x*.

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

# Disabling LDAP Authentication

If you permanently disable LDAP authentication, users sign in to Unity Connection web applications by using their Unity Connection web application password instead of their LDAP directory password. If Unity Connection users were integrated with an LDAP directory when Unity Connection was first installed or if they have been integrated with an LDAP directory for a while, they either do not have Unity Connection web application passwords or they do not remember their Unity Connection web application password. Do the following procedure to force users to change their Unity Connection web application password the next time they sign in to a Unity Connection web application and to disable LDAP authentication.

You can use Bulk Edit to change passwords for users who have a mailbox, but you must individually change passwords for users who not have a mailbox (meaning administrators).

If you temporarily disable LDAP authentication, for example, because you are changing which field is mapped to the Alias field in Unity Connection, you do not have to change password settings for Unity Connection users.

### To Disable LDAP Authentication

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

**Step 2** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, and select **LDAP Authentication**.

**Step 3** Uncheck the **Use LDAP Authentication for End Users** check box.

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

**Step 5** If you are only temporarily disabling LDAP authentication, skip the rest of this procedure. Do not change password settings.

**Step 6** To change the password setting for users who have a mailbox:

a. In Cisco Unity Connection Administration, expand **Users** and select **Users**.

b. If all Unity Connection users are integrated with LDAP directory users, select all users. Otherwise, select the users who are integrated with an LDAP directory.

c. Select **Bulk Edit**.

d. On the **Edit** menu, select **Password Settings**.

e. In the **Choose Password** list, choose **Web Application**.

f. For **User Must Change at Next Sign-In**, check both check boxes.

g. If you want to schedule when Unity Connection changes the setting for the selected users, under **Bulk Edit Task Scheduling,** choose **Run Later** and specify a date and time.

h. Select **Submit**.

**Step 7** To change the password setting for users who do not have a mailbox:

a. In Cisco Unity Connection Administration, expand **Users** and select **Users**.

b. Select the first user.

c. On the **Edit** menu, select **Password Settings**.

d. In the **Choose Password** list, choose **Web Application**.

e. Check the **User Must Change at Next Sign-In** check box.

f. Select **Save**.

g. Repeat Step a. through Step f. for the remaining users who do not have a mailbox.

# Selecting the LDAP Users to Import into Cisco Unity Connection 10.x

Later in this chapter, you create up to five Cisco Unity Connection LDAP directory configurations that specify which users in the LDAP directory you want to import into Unity Connection. For each LDAP directory configuration, you specify a user search base, which is the position in the LDAP directory tree where Unity Connection begins its search for user accounts. Unity Connection imports all users in the tree or subtree (domain or OU) specified by the search base. A Unity Connection server or cluster can only import LDAP data from subtrees with the same directory root, for example, from the same Active Directory forest.

After you create the LDAP directory configurations, you synchronize Unity Connection data with data in the LDAP directory, which imports LDAP data into a hidden Cisco Unified Communications Manager database on the Unity Connection server. There is a practical limit of 60,000 users that can be imported into the Cisco Unified CM database. The limit is not enforced by the synchronization process, but importing large numbers of LDAP users who will not become Unity Connection users reduces the amount of disk space available for messages, slows database performance, and causes upgrades to take longer.

**Caution** Do not specify user search bases that will cause more than 60,000 users to be imported into the Cisco Unified CM database during synchronization, or Unity Connection performance will be adversely affected.

We recommend that you analyze the structure of your LDAP directory and determine whether you can specify five or fewer user search bases that:

- Include the LDAP users that you want to import into Unity Connection.
- Exclude the LDAP users that you do not want to import into Unity Connection.
- Will cause fewer than 60,000 users to be imported into the Cisco Unified CM database.

If you cannot specify five or fewer search bases that meet all three of these criteria, we recommend that you create one or more LDAP filters to filter out the unwanted users specified by the search bases. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 10.x" section on page 44-12.

## Directories Other than Active Directory

If you are using an LDAP directory other than Microsoft Active Directory, and if you create a Unity Connection LDAP directory configuration that specifies the root of the directory as the user search base, Unity Connection will import data for every user in the directory. If the root of the directory contains subtrees that you do not want Unity Connection to access (for example, a subtree for service accounts), do one of the following:

- Create two or more Unity Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Unity Connection to access.
- Create an LDAP search filter. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 10.x" section on page 44-12.

For directories other than Active Directory, we recommend that you specify user search bases that include the smallest possible number of users to speed synchronization, even when that means creating multiple configurations.

## Active Directory

If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; Unity Connection does not follow Active Directory referrals during synchronization. The same is true for an Active Directory forest that contains multiple trees—you must create at least one configuration to access each tree. In this configuration, you must map the UserPrincipalName (UPN) attribute to the Unity Connection Alias field; the UPN is guaranteed by Active Directory to be unique across the forest.

## Cisco Unity Connection Intrasite and Intersite Networking

If you are using intrasite or intersite networking to network two or more Unity Connection servers that are each integrated with an LDAP directory, and if you specify a user search base on one Unity Connection server that overlaps a user search base on another Unity Connection server, be careful not to accidentally create duplicate Unity Connection users on different Unity Connection servers by importing the same LDAP user more than once.

**Note** Regardless of how you create users, Unity Connection prevents you from creating two users with the same alias on the same Unity Connection server, but does not prevent you from creating two users with the same alias on different Unity Connection servers in the same site or organization.

In some cases, you may find it useful to create multiple Unity Connection users from the same LDAP user. For example, you may want to import the same LDAP administrator accounts into every Unity Connection server as Unity Connection users without voice mailboxes, and use these duplicate Unity Connection users as administrator accounts. This allows you to use LDAP synchronization and authentication for Unity Connection administrator accounts without creating one or more LDAP users for every Unity Connection server.

# Filtering LDAP Users in Cisco Unity Connection 10.x

You may want additional control over which LDAP users you import into Cisco Unity Connection for a variety of reasons. For example:

- The LDAP directory has a flat structure that you cannot control sufficiently by specifying user search bases.
- You only want a subset of LDAP user accounts to become Unity Connection users.
- The LDAP directory structure does not match the way you want to import users into Unity Connection. For example:
  - If organizational units are set up according to an organizational hierarchy but users are mapped to Unity Connection by geographical location, there might be little overlap between the two.
  - If all users in the directory are in one tree or domain but you want to install more than one Unity Connection server, you need to do something to prevent users from having mailboxes on more than one Unity Connection server.
- The LDAP directory includes more than 60,000 users. When you create Unity Connection users by importing LDAP users, there is a practical limit of 60,000 users that can be imported into the Cisco Unified Communications Manager database on the Unity Connection server. The limit is not enforced by the synchronization process, but importing large numbers of LDAP users who will not become Unity Connection users slows database performance and causes upgrades to take longer.

In these cases, you may want to create one or more LDAP filters to provide additional control over user search bases. Note the following:

- You cannot create LDAP filters for Cisco Unified Communications Manager Business Edition.
- You can create as many LDAP filters as you want, but you can only have one active filter per Unity Connection directory configuration, up to five per server or cluster.
- When you create LDAP directory configurations in Unity Connection, you specify both a user search base and an LDAP filter. As applicable, create filters that integrate with the user search bases that you will specify for the maximum of five LDAP directory configurations that you can create.

- Each filter must adhere to the LDAP filter syntax specified in RFC 4515, "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters."
- The filter syntax is not validated when you create the filter. Instead, it is validated when you specify the filter in an LDAP directory configuration.
- If you add a filter and add it to an LDAP directory configuration that you have already synchronized with the LDAP directory, or if you change a filter that is already in use in an LDAP directory configuration, you must do the following steps for the LDAP users specified by the new or updated filter to be accessible to Unity Connection:
  1. Turn off and turn on again the Cisco DirSync service. In Cisco Unified Serviceability, select **Tools > Service Activation**. Uncheck the check box next to **Cisco DirSync**, and select **Save** to turn off the service. Then check the check box next to **Cisco DirSync**, and select **Save** to turn on the service.
  2. In Connection Administration, in the LDAP directory configuration that accesses the filter, perform a full synchronization (select **Perform Full Sync Now**).
- If you change a filter to one that excludes some of the users who were previously accessible, the Unity Connection users who are synchronized with the now-inaccessible LDAP users will be converted to standalone Unity Connection users over the next two scheduled synchronizations or within 24 hours, whichever is greater. The users will still be able to sign in to Unity Connection by phone, callers can still leave messages for them, and their messages will not be deleted. However, they will not be able to sign in to Unity Connection web applications while Unity Connection is breaking synchronization for these users. After the synchronization has been broken, their web-application passwords will be the passwords that were assigned when their Unity Connection accounts were created.

Do the following procedure to add an LDAP filter.

#### To Add an LDAP Filter

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then select **LDAP Custom Filter**.

**Step 2** Select **Add New**.

**Step 3** In the **Filter Name** field, enter a name for this LDAP filter. If you are adding more than one LDAP filter configuration, enter a name that identifies the LDAP users included in the current filter, for example, "Engineering."

**Step 4** In the **Filter** field, enter a filter that adheres to the LDAP filter syntax specified in RFC 2254, "The String Representation of LDAP Search Filters." You must enclose the filter text in parentheses.

**Step 5** Select **Save**.

# Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x

**Note** If you are configuring unified messaging with Exchange, you must enter the Exchange email address for each Unity Connection user. On the Unified Messaging Account page in Connection Administration, each user can be configured to use either of the following values:

– The Corporate Email Address specified on the User Basics page
– The email address specified on the Unified Messaging Account page

As you add LDAP directory configurations, we recommend that you choose the option to synchronize the Mail ID field in Cisco Unified Communications Manager with the mail field in the LDAP directory. This causes values in the LDAP mail field to appear in the Corporate Email Address field in Unity Connection. Automatically populating the Corporate Email Address field with the value of the LDAP mail field is easier than populating the email address field on the Unified Messaging Account page by using Connection Administration or the Bulk Administration Tool.

Do the following procedure once for each user search base in the LDAP directory from which you want to import user data into Cisco Unity Connection.

### To Add an LDAP Directory Configuration

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

**Step 2** In the **LDAP Configuration Name** field, enter a name for this LDAP directory configuration. If you are adding more than one LDAP directory configuration with different LDAP user search bases, enter a name that identifies the users in the current search base.

**Step 3** Enter other values as applicable. For more information, on the Help menu, select **This Page**.

If you specify an LDAP filter, LDAP filter syntax is checked. If the syntax is invalid, an error message appears.

If you uploaded SSL certificates to the Unity Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 44-7, check the **Use SSL** check box for every LDAP server that you specify in the **Host Name or IP Address for Server** field.

**Note** With some supported LDAP directories, you cannot specify redundant LDAP servers. For information on the LDAP directories with which Unity Connection allows you to specify redundant servers, see the "Requirements for an LDAP Directory Integration" section in *System Requirements for Cisco Unity Connection Release 10.x*.

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

**Step 5** Select **Perform Full Sync Now**.

**Step 6** To add another LDAP directory configuration for another user search base, select **Add New**, and repeat Step 2 through Step 5

**Note** When importing users from LDAP, the user gets successfully imported into the enduser table. However, w hen the user is imported into the tbl_user from enduser table, the sync fails if the middlename has value more than 12 bytes.

# Changing LDAP Directory Configurations in Cisco Unity Connection 10.x

If you want to change an LDAP directory configuration, for example, by changing which LDAP user fields are imported into Unity Connection, you must delete the existing directory configuration and recreate it.

**Caution** You must recreate the directory configuration within 24 hours, or the Unity Connection users that are integrated with LDAP users will be converted to standalone Unity Connection users.

### To Change LDAP Directory Configurations

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the **System Administrator** role.

**Step 2** Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

**Step 3** If you do not have a record of the existing settings, select the configuration that you want to change, and write down the existing settings.

**Step 4** On the **Find and List LDAP Directory Configurations** page, check the check box next to the directory configuration that you want to change.

**Note** If the directory configuration does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 5** Select **Delete Selected**.

**Step 6** In the dialog box that opens, asking you to confirm the deletion, select **OK**.

**Step 7** Under **System Settings > LDAP**, select **LDAP Setup**.

**Step 8** On the **LDAP Setup** page, uncheck the **Enable Synchronizing from LDAP Server** check box.

**Step 9** Select **Save**.

**Step 10** Recheck the **Enable Synchronizing from LDAP Server** check box.

**Step 11** Select **Save** again.

**Step 12** Recreate the directory configuration, and perform a full synchronization for the recreated directory configuration. See the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x" section on page 44-14.

**Step 13** Repeat Step 2 through Step 12 for other directory configurations that you want to change, if any.

# Deleting LDAP Directory Configurations in Cisco Unity Connection 10.x

If you want to delete an LDAP directory configuration, for example, because you no longer want Unity Connection users to be integrated with an LDAP directory, do the following procedure.

**Caution** When you delete a directory configuration, Unity Connection users that are integrated with LDAP users are converted to standalone Unity Connection users in 24 hours.

### To Delete LDAP Directory Configurations

**Step 1** Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

**Step 2** Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

**Step 3** On the **Find and List LDAP Directory Configurations** page, check the check boxes next to the directory configurations that you want to delete.

**Note** If a directory configuration does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

**Step 4** Select **Delete Selected**.

**Step 5** In the dialog box that opens, asking you to confirm the deletion, select **OK**.

**Step 6** Under **System Settings > LDAP**, select **LDAP Setup**.

**Step 7** On the **LDAP Setup** page, uncheck the **Enable Synchronizing from LDAP Server** check box.

**Step 8** Select **Save**.

**Step 9** Recheck the **Enable Synchronizing from LDAP Server** check box.

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

# Changing Which LDAP Field Is Mapped to the Alias Field in Unity Connection

If you need to change which field in the LDAP directory is mapped to the Alias field in Unity Connection, do the following procedure.

**Caution** You must complete this entire procedure within 24 hours, or Unity Connection will convert all of the users who are integrated with the LDAP directory to standalone Unity Connection users.

**Caution** If you are using LDAP authentication, after you complete this procedure, users will have to sign in to Unity Connection web interfaces by using the new value of the Alias field in Unity Connection.

### To Change the LDAP Field that Is Mapped to the Alias Field in Unity Connection

**Step 1** Disable the DirSync service:

a. Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

b. On the **Tools** menu, select **Service Activation**.

c. Under **Directory Services,** uncheck the **Cisco DirSync Service** check box.

d. Select **Save**, and select **OK** to confirm.

**Step 2** Disable LDAP authentication. See the "Disabling LDAP Authentication" section on page 44-9.

**Step 3** Delete all LDAP directory configurations:

a. Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

b. Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

c. If necessary, write down the specifications for the existing LDAP directory configurations so you can reproduce them later in this procedure.

d. On the **Find and List LDAP Directory Configurations** page, select all directory configurations.

e. Select **Delete Selected**.

**Step 4** Change the field that is mapped to the Unity Connection **Alias** field:

a. In Connection Administration, expand **System Settings > LDAP**, then select **LDAP Setup**.

b. In the **LDAP Attribute for User ID** list, select the field in the LDAP directory whose data you want to appear in the **Alias** field in Unity Connection. Note the following requirements:

- The field that you select must have a value for every user in the LDAP directory.
- Every value for that field must be unique.

**Caution** If you select a field other than sAMAccountName, when users sign in to the Cisco PCA or an IMAP client (Unity Connection 10.x) or sign in to the Web Inbox, they must enter their Unity Connection alias and their LDAP password.

c. Select **Save**.

**Step 5** Re-enable LDAP authentication. For more information, see the "Configuring LDAP Authentication in Cisco Unity Connection 10.x" section on page 44-8.

**Step 6** Re-add LDAP configurations, but do not synchronize Unity Connection and LDAP data. The synchronization will not work until after you re-enable the DirSync service in the next step.

For more information, see the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 10.x" section on page 44-14.

**Step 7** Re-enable the DirSync service:

a. Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

b. On the Tools menu, select **Service Activation**.

c. Under Directory Services, check the **Cisco DirSync Service** check box.

d. Select **Save**, and select **OK** to confirm.

**Step 8** Synchronize Unity Connection data with LDAP data:

a. In Connection Administration, expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

b. Select **Find** to display a list of all directory configurations.

c. Display the first directory configuration, and select **Perform Full Sync Now**.

d. Repeat Step a. through Step c. for the remaining directory configurations.

# Setting up Tenant Partitioning in Cisco Unity Connection 10.x

## Introduction to Tenant Partitioning

In Cisco Unity Connection 9.1 and earlier releases, Unity Connection could provide voicemail solution to one enterprise on a single installation. Starting with Unity Connection 10.0 release, a concept of tenant partitioning has been introduced where administrator can configure multiple SMBs as tenants on a single Unity Connection installation.

Each tenant has its own set of partition, schedule set, schedule, schedule detail, search space, search space member, phone system, class of service, user template, distribution list, distribution list membership, user operator, call handler template, directory handler, interview handler, call handlers (operator, opening greeting, GoodBye), and routing rules. The following configuration objects are shared across multiple tenants:

All the system settings like mailbox store, custom keypad, restriction tables etc. are shared across the multiple tenants.

Tenant partitioning also introduces the concept of using the corporate email addresses as their alias, which enables alias uniqueness across tenants. To achieve this, the aliases assigned to the users (in multi-tenancy environment) must be in the form of alias@smtpdomain, which would be the corporate email address of the tenant's user. To login into the Unity Connection User Web interfaces like Cisco PCA, Web Inbox, VMREST API, users have to use this alias format. Two different tenants configured on the same Unity Connection can never have the same alias for their users as the smtp domain will always differ.

**Note** There are no changes done for touchtone conversation and voice-recognition users.

## Tenant Provisioning using APIs

Cisco Unity Connection Provisioning Interface (CUPI) provides set of APIs for Cisco Unity Connection that can be used for tenant provisioning. To support the Tenant Partitioning using APIs in Unity Connection, few new APIs have been developed and few existing APIs have been modified.

For more information about provisioning APIs, see the Documentation Wiki:
http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Provisioning_Interface_%28CUPI%29_API

# Working with Tenant Partitioning

The following steps list the basic configuration settings to provision a tenant:

**Step 1** **Create Tenant:** A new API has been introduced for tenant provisioning. All its associated objects are created by executing a single API request. If the operation fails at any point in time, the entire process is rolled back. To create a tenant, an HTTP POST request should be sent to the URI:

https://<connection-server>/vmrest/tenants

For the optional parameters, if no value is specified then system default values will be used.

**Step 2** **Create Port Group:** To create a port group, an HTTP POST request should be sent to the URI:

https://<connection-server>/vmrest/portgroups

Tenant partitioning supports SIP integration only.

**Step 3** **Create Ports:** To create a port, an HTTP POST request should be sent to the URI:

https://<connection-server>/vmrest/ports

**Step 4** **Integrate with Call Manager:** To integrate with Call Manager, do the following:

- Create SIP Security Profile
- Create SIP Profile
- Create Trunk to Publisher and Subscriber
- Create Route Group
- Create Route List
- Create Route Pattern
- Create Voicemail Pilot and Voicemail Profile

**Step 5** **Create User for the Tenant:** To create a user, an HTTP POST request should be sent to the URI:

https://<connection-server>/vmrest/users?templateAlias=<TenantUserTemplate>

User template specified in the URI should belong to the tenant for which you are creating the user.

**Step 6** **Record Greetings:** To record the greetings, do the following:

- Create a temporary place-holder WAV file on Unity Connection via POST operation on the URI:

https://<connection-server>/vmrest/voicefiles

- Use the temporary file name created before to upload the new audio. The HTTP content type is "audio/wav" and the payload content is the audio data.

PUT https://<connection-server>/vmrest/voicefiles/<TemporaryFileName>

- Assign temporary audio WAV file to the target resource. Perform a POST operation on the following URI:

https://<connection-server>/vmrest/handlers/callhandlers/<TenantCallHandlerObjectId>/greetings/Standard/greetingstreamfiles/1033

**Step 7** **Call Pilot Number:** Dial the pilot number. You will hear the recorded opening greeting.

For more information about provisioning APIs, see the Documentation Wiki:

http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Provisioning_Interface_%28CUPI%29_API

# Phone System Integration

For multiple phone systems integration with Cisco Unity Connection, see the Multiple Phone System Integration Guide for Cisco Unity Connection Release 10.x available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/integration/guide/multiple_integration/cuc10xintmultiple.html.

# Modifying the Objects after Tenant Creation

The administrator can modify the objects associated with a tenant after its creation. For example, to add new routing rule for a tenant, do the following steps:

**Step 1** Create a new routing rule, by sending the below POST request:

POST https://<connection-server>/vmrest/routingrules

Set the search space for the routing rule as per the tenant's search space for which this routing rule is getting created.

**Step 2** Create a new routing rule condition, by sending the below POST request:

POST https://<connection-server>/vmrest/routingrules/<routingrulesobjectId>/routingruleconditions

Add the tenant's phone system as the routing rule condition.

# Managing Licenses in Cisco Unity Connection 10.x

See the following sections:


- About Licenses in Cisco Unity Connection 10.x, page 46-1
- Viewing Reports for Licenses in Cisco Unity Connection 10.x, page 46-3


# About Licenses in Cisco Unity Connection 10.x

See the following sections:


- License Management and Enterprise License Manager (ELM) in Cisco Unity Connection 10.x, page 46-1
- Licenses and Cisco Unity Connection Clusters, page 46-3
- Licenses and Migrations from Cisco Unity, page 46-3


## License Management and Enterprise License Manager (ELM) in Cisco Unity Connection 10.x

In Cisco Unity Connection 10.x, licenses are required to use the various features purchased by the customers. To use the licensed features on Unity Connection, the licenses for the corresponding features must be installed on the Enterprise License Manager (ELM) server and Unity Connection must communicate with the ELM server to obtain the license status. The ELM server provides centralized, simplified, and enterprise-wide management of user-based licensing. For more information on the ELM server and its configuration, refer to ELM user guide at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/elmuserguide/10x/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html.

Cisco Unity Connection remains in the “Demonstration (Demo)” mode until it connects with the ELM server for the first time. For more information on licensing states of Unity Connection, refer to the License Status in Cisco Unity Connection, page 46-2.

## Obtaining and Installing the Licenses

For details on obtaining and installing the licenses in the ELM server, see the "*New License Fulfillment*" section in the ELM user guide at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/elmuserguide/10x/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html.

After obtaining and installing the licenses, you are required to configure Unity Connection with the ELM server. For information on how to connect Unity Connection with the ELM server, refer to the "*Adding a Product instance*" section in the ELM user guide. After Unity Connection is configured with the ELM server, Unity Connection is no longer in “Demo” mode. To check the details of the connected ELM server, see the "**Status**" section on the License page of Cisco Unity Connection Administration. The value of the ELM server is displayed as “Not Connected” on the **License** page until Unity Connection is configured on the ELM server.

## License Status in Cisco Unity Connection

When Cisco Unity Connection is connected with the ELM server and the required number of licenses for the features are installed on the ELM server, the license status becomes “Compliance”. For example, if the ELM server is configured for 50 users, the Unity Connection server can request for less than equal to 50 users to remain in “Compliance” mode.

If the required number of licenses are not installed on the ELM server, the license status becomes “Violation”. However, you can still use the licensed features on Unity Connection for 60 days, which is the grace period. During this grace period, you are required to obtain and install the required number of licenses or reduce the usage of the licensed features in order to avoid license violation. However, if you do not take the required action during the grace period, then license status becomes “Expire”.

Once the license status of Cisco Unity Connection software changes to “Expire”, the software will stop functioning. The Unity Connection server will not answer any calls to leave or retrieve voicemails. However, you can still add, modify or delete configuration data on the server. You are required to obtain and install the required number of licenses or reduce the usage of the licensed features to avoid license violation. After taking the required action, the license status changes from “Expire” to “Compliance” and you can use the licensed features on Unity Connection again.

**Note** After obtaining and installing licenses for changing the license status from “Expire” to the “Compliance”, you must restart Cisco Unity Connection.

**Note** When the license status of Unity Connection is “Expire”, the synchronization of users and call handler profiles from Unity Connection on the branch stops working. However, the voicemail and auto-attendant functionalities still work at branch. For more information on the licensing requirements of the branch, refer to the *Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) Guide for* Cisco Unity Connection*Release 10.x* at guide http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/srsv/guide/10xcucsrsvx.html.

You can view the license status on the License page of the Cisco Unity Connection Administration. For more information, see the “Viewing the License Status for Cisco Unity Connection” section in this document.

**Note** If the multiple Unity Connection severs are configured with the same ELM server and the license violation occurs for one of the Unity Connection, then the license status of all the Unity Connection servers becomes “Violation”. Similarly, if the license expiration occurs for one of the Unity Connection, then the license status of all the Unity Connection servers becomes “Expire”.

## Licenses and Cisco Unity Connection Clusters

In a Cisco Unity Connection (high availability) environment, only the publisher server needs to be configured and connected with the ELM to obtain the license status and for the license enforcement. When the publisher server stops functioning (for example, when it is shut down for maintenance), the subscriber server handles all the incoming calls for the cluster for 60 days grace period. However, if the publisher server does not resume its normal function within the 60 days grace period, Unity Connection will move to “Expire” state.

## Licenses and Migrations from Cisco Unity

Cisco Unity Connection 10.x can use existing license information from Cisco Unity to enable Cisco Unity Connection features when migrating from Cisco Unity 4.x or later to Unity Connection 10.x.

For instructions on migrating from Cisco Unity 4.x or later to Cisco Unity Connection 10.x, see the “Migrating from Cisco Unity 4.x or Later to Cisco Unity Connection 10.x” chapter of the *Upgrade Guide for Cisco Unity Connection Release 10.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/elmuserguide/10x/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html.

**Note** Before starting migration, you need to configure Unity Connection with the ELM server. For more information on configuring Unity Connection with the ELM server, refer to the ELM user guide at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/elmuserguide/10x/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html.

# Viewing Reports for Licenses in Cisco Unity Connection 10.x

You can view the reports for the licenses associated with the licensed features on the **License** page of the Cisco Unity Connection Administration. The license report includes the following information:

- **Status**: Shows the license status, host name/IP address of the connected ELM server, last connectivity time of Unity Connection with the ELM server, and last compliance time of Unity Connection with the ELM server.
- **License Usage**: Shows the usage of licensed features of the Unity Connection server. For features that are licensed for a number of seats, the report displays the number of used seats.

## Viewing the License Status for Cisco Unity Connection

Do the following procedure to view the license status for the Cisco Unity Connection server.

#### To View the License Status for Cisco Unity Connection

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Licenses**.

**Step 2** On the **Licenses** page, under **Status**, you can view the following types of License status:

- **Demonstration (Demo)**: If Unity Connection is in the "Demo" mode, the value of License status will be "Demo".
- **Compliance**: If the required number of licenses for the desired feature are installed on the ELM server, the Unity Connection is in the "Compliance" mode.
- **Violation**: If required number of licenses for the desired feature are not installed on the ELM server, the License status becomes "Violation". In addition, a warning message stating "License Violation has occurred. License will expire in 60 day(s). Please contact ELM administrator" appears.
- **Expire**: If you do not obtain and install the required number of licenses for the desired features on the ELM server within the 60 days grace period, the license status becomes "Expire". A warning message stating "**License violation has occurred for x day(s) and crossed the grace period. System is now in Expiration mode**" appears, where "x" is the number of days. In addition, a warning message stating "**Cisco Unity Connection cannot answer calls. A license violation has occurred. To review licenses, go to the System Settings > Licenses page in Cisco Unity Connection Administration**" appears on the Home page of the Cisco Unity Connection Administration.

## Viewing the Last Connectivity Time with the ELM Server

Do the following procedure to view the Last Connectivity Time with the ELM Server.

#### To View the Last Connectivity Time with the ELM Server

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Licenses**.

**Step 2** On the Licenses page, under Status, the value of the Last Connectivity Time of Unity Connection with the ELM server is displayed.

**Note** The value of the Last Connectivity Time with ELM Server will be in Coordinated Universal Time (UTC) time zone.

## Viewing the Host Name/ IP Address of the Connected ELM Server

#### To View the Host Name/ IP Address of the Connected ELM Server

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Licenses**.

**Step 2** On the **Licenses** page, under **Status,** the Host name/ IP address of the Connected ELM server is displayed.

# Viewing the Last Compliance Time

**To View the Last Compliance Time of the Cisco Unity Connection**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Licenses**.

**Step 2** On the **Licenses** page, under **Status**, the value of the last compliance time of Unity Connection with ELM server is displayed.

**Note** The value of the Last Compliance Time will be in Coordinated Universal Time (UTC) time zone.

# Viewing the License Usage

**To View the License Usage for Cisco Unity Connection**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then select **Licenses**.

**Step 2** On the Licenses page, under **License Usage**, the license usage for the Unity Connection server is displayed in the "**Current usage**" column.

# License Parameters for Cisco Unity Connection 10.x Features

*Table 46-1 License Parameters for Cisco Unity Connection Features*

| License Parameter | Feature | Description |
|---|---|---|
| CUC_BasicMessaging | Total number of voicemail users | Specifies the maximum number of voice mail users configured in Cisco Unity Connection |
| CUC_SpeechView | Total number of speech view standard users | Specifies the maximum number of Speech view Standard users configured in Cisco Unity Connection |
| CUC_SpeechViewPro | Total number of speech view professional users | Specifies the maximum number of Speech view Professional users configured in Cisco Unity Connection |
| CUC_SpeechConnectPort | Total number of speech connect ports | Specifies the maximum number of Speech Connect calls configured in Cisco Unity Connection |

*Table 46-1 License Parameters for Cisco Unity Connection Features (continued)*

| License Parameter | Feature | Description |
|---|---|---|
| CUC_EnhancedMessaging | Total number of enhanced messaging users | Specifies the maximum number of Unity Connection SRSV users configured on Cisco Unity Connection. The Unity Connection SRSV users are reflected under this tag only when the branch is active. |

# Managing Cisco Unity Connection Survivable Remote Site Voicemail in Cisco Unity Connection 10.x

See the following sections:


- Overview of Cisco Unity Connection SRSV in Unity Connection 10.x, page 47-1
- Working with Unity Connection SRSV, page 47-2
- Managing Branches in Cisco Unity Connection 10.x, page 47-6


## Overview of Cisco Unity Connection SRSV in Unity Connection 10.x

Cisco Unity Connection Survivable Remote Site Voicemail (Unity Connection SRSV) is a backup voicemail solution that allows you to receive voice messages during WAN outages. It works in conjunction with Cisco Unified Survivable Remote Site Telephony (SRST) for providing voicemail service to a branch when the connectivity with the central Unity Connection voicemail service is lost.

Unity Connection SRSV is used in the centralized Cisco Unified Communications Manager and Cisco Unity Connection environment with multiple branch offices or small sites. It provides limited voicemail and auto-attendant features that remain in synchronization with the central Unity Connection voicemail service so that when the WAN outage or failure occurs, the Unity Connection SRSV solution can provide voicemail service to the subscribers at the branch. However, as soon as the network is restored, all the voicemails received by the branch subscribers are automatically uploaded to the central Unity Connection voicemail server.

Unity Connection SRSV solution requires the following two components:

- Cisco Unity Connection: It is deployed at the central site alongside with Cisco Unified CM to deliver powerful integrated messaging and voicemail services.
- Unity Connection SRSV: The SRSV component is natively a part of Unity Connection which is deployed at the branch site alongside with Cisco Unified CM Express or Cisco Unified Survivable Remote Site Telephony (SRST). Unity Connection SRSV is hosted on Cisco Integrated Service Routers Generation 2 (ISR G2) platform by using Services Ready Engine Virtualization.

Unity Connection SRSV is a licensed feature for which you need to install licenses under **CUC_EnhancedMessaging** tag on the **License** page of Cisco Unity Connection Administration. For more information on licenses installed on the central Unity Connection server, refer to the "Managing

Licenses in Cisco Unity Connection 10.x" chapter of the System Administration Guide for Cisco Unity Connection Release 10.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx.html.

See the following sections:

- Working with Unity Connection SRSV, page 47-2
- Managing Branches in Cisco Unity Connection 10.x, page 47-6

# Working with Unity Connection SRSV

Unity Connection SRSV comes into picture during WAN outages and acts as a backup of voice messaging system at the branch sites. It allows the users at branch offices to receive the voice messages during WAN outages.

In Unity Connection 10.x, Unity Connection SRSV involves provisioning of Unity Connection through the command line interface (CLI) to run it in SRSV mode, SRST/E-SRST references Cisco Unified Communications Manager, and all the SRSV related functionalities, such as user(s) provisioning and voicemail upload, are managed by the central Unity Connection server. Once the entire Unity Connection SRSV system is deployed and provisioned, it remains in the idle state at the branch site and is ready to receive calls from the SRST system (either SRST or CUCME-as-SRST). The SRST component also remains idle and wait for IP phones to register with it. When the WAN outage occurs, the branch office IP phones that are registered to the central Cisco Unified Communications Manager detect the loss of connectivity and re-home to the SRST. Now, all the incoming calls to the branch are handled by the SRST. For calls that are either no-answer or reach a busy line, SRST forwards the call to the CUC-SRSV voicemail server that allows the caller to leave a voice message for the branch user. As a result, the branch office voicemail is supported during WAN outages when the central office voicemail system is unreachable.

However, when the WAN Unity Connection is restored, the IP phones automatically re-home to the central Cisco Unified Communications Manager. All the call are then managed by Cisco Unified Communications Manager and the no-answer / busy calls are forwarded to the central Unity Connection voicemail system and all the voicemails stored on the branch get automatically synchronized with the central Unity Connection voicemail.

See the following sections:

- Supported SRSV Topologies, page 47-2
- Methods of Provisioning and Voicemail Upload, page 47-5
- Configuring an SRSV User, page 47-6

## Supported SRSV Topologies

Unity Connection SRSV supports several topologies based on the configuration of the router. You can deploy either original SRST or CUCME-as-SRST (also known as SRST Fallback Mode) at branch.

**Note** If you are running SRST at the branch site, you cannot also deploy the E-SRST feature.

Following figures show three topologies supported by Unity Connection SRSV:

Figure 47-1: Shows a topology in which SRST is deployed at the branch site. If the WAN outage occurs or PSTN goes down, Unity Connection SRSV at the branch site provides limited voicemail support in the failover mode.

Figure 47-2: Shows a topology where CUCME-as-SRST (also known as SRST Fallback Mode) is providing call control at the branch site.

Figure 47-3: Shows a topology where multiple CUCME-as-SRST and SRSV-CUE devices are paired for load balancing at the survivable branch site. In this scenario, the administrator uses Cisco Unified Communications Manager to divide the branch users between CUCME-SRST-1 and CUCME-SRST-2. The central Unity Connection server detects that and then sends the appropriate configuration to SRSV-1 and SRSV-2 at the branch site. In the event of WAN failure, each SRSV device will handle calls directed to it from the paired CUCME-as-SRST device.

***Figure 47-1 Topology 1***

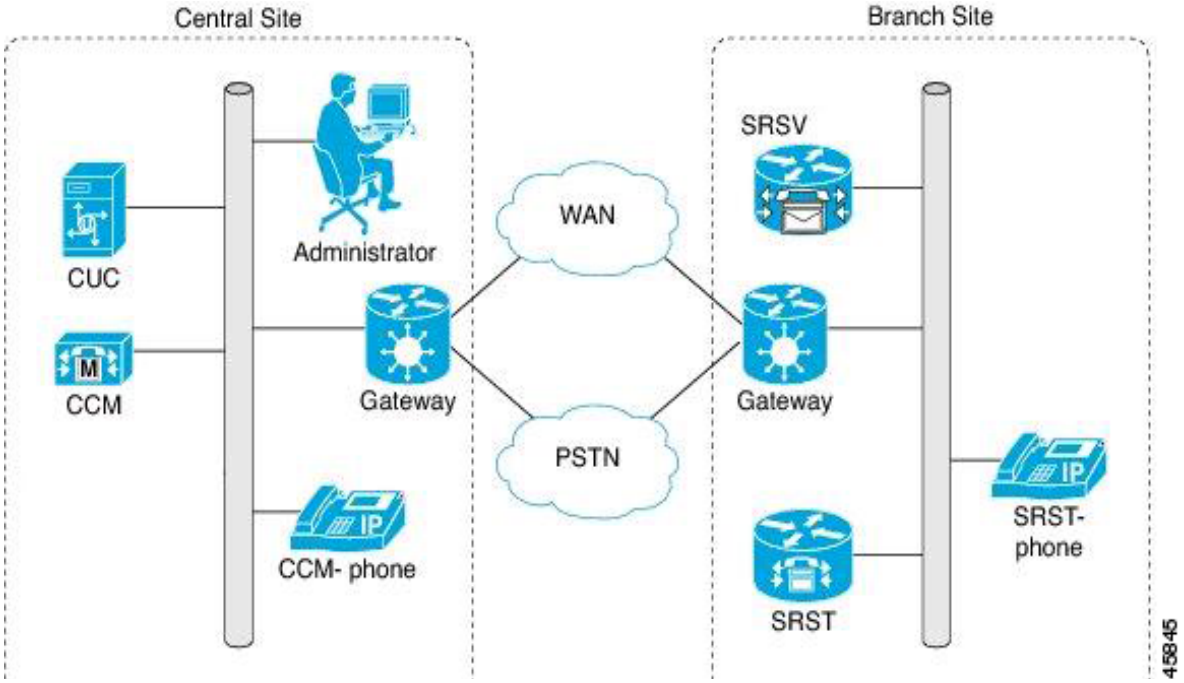


*Figure 47-2 Topology 2*

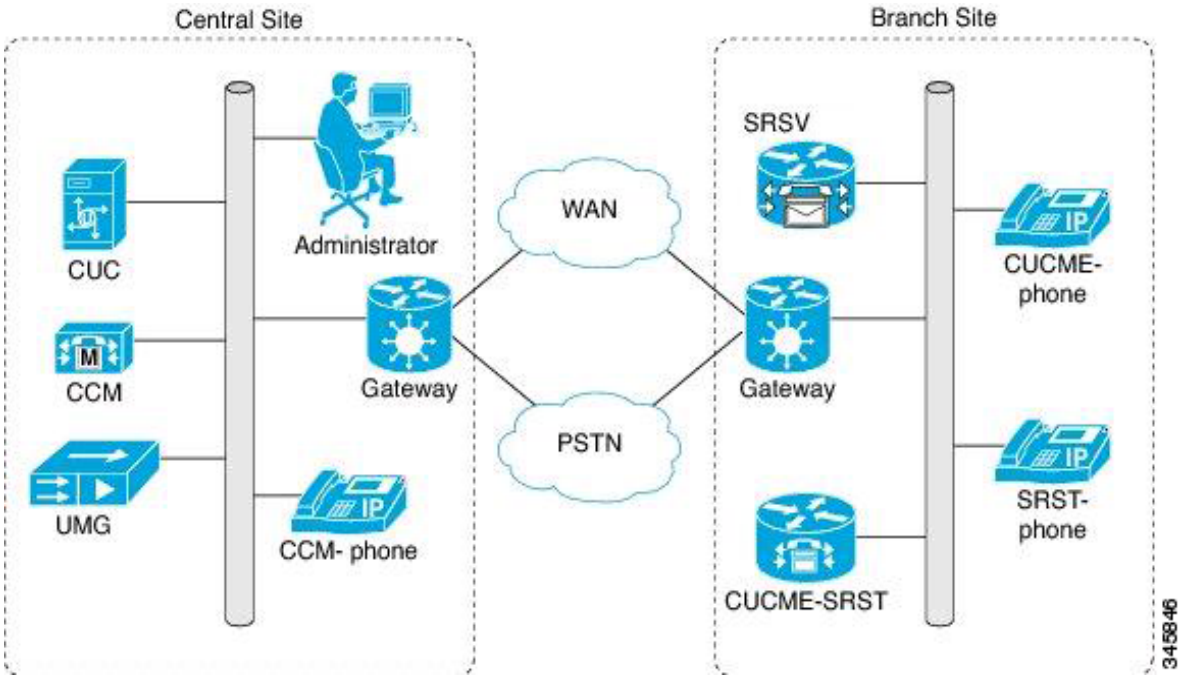
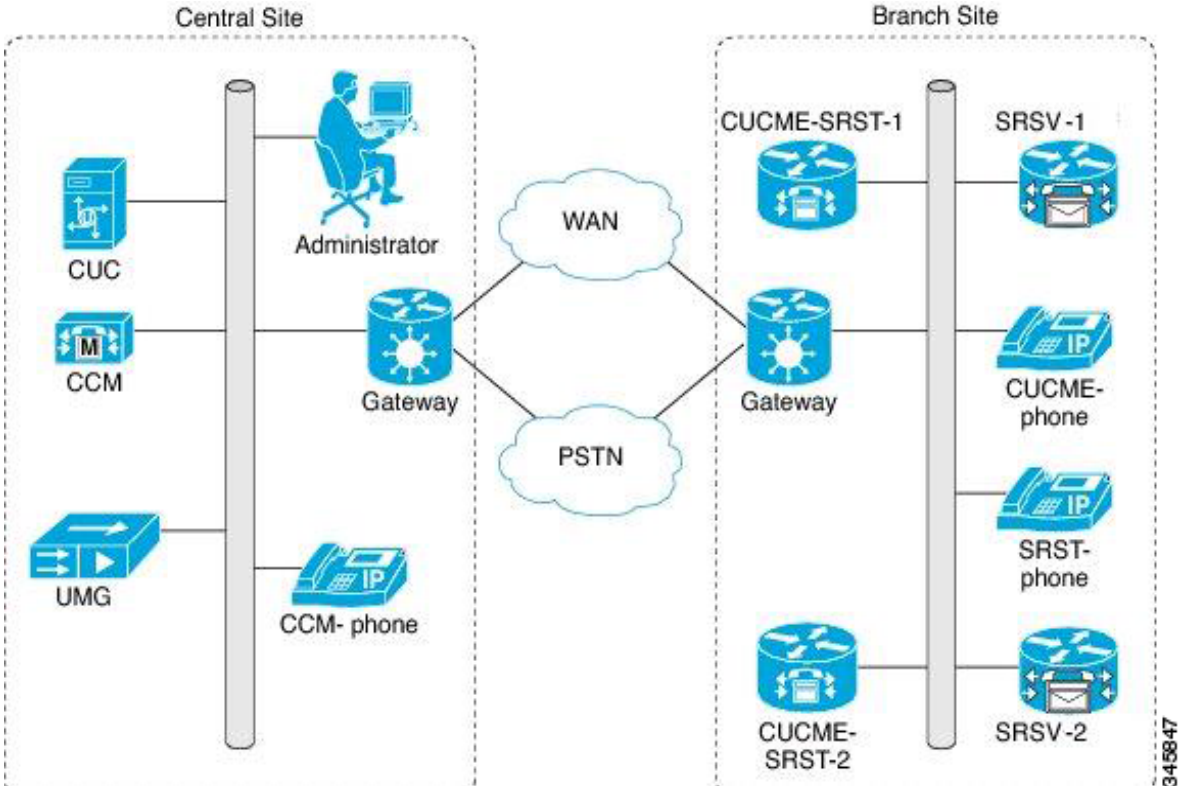



*Figure 47-3 Topology 3*



**Note** You can still install UMG in the network for E-SRST.

See also:

- Methods of Provisioning and Voicemail Upload, page 47-5
- Task List to create an Unity Connection SRSV User, page 47-6

# Methods of Provisioning and Voicemail Upload

Unity Connection 10.x supports two methods for provisioning and voicemail upload between Unity Connection and Unity Connection SRSV. You can use either of the following methods to provision the users from the central Unity Connection server to the branch system:

- **Manual Synchronization of Provisioning**: To manually provision the users on the branch, navigate to **Branch Management > Edit Branch** on Cisco Unity Connection Administration (CUCA) and select **Sync Provisioning**.
- **Automatic Synchronization of Provisioning**: To automatically enable the provisioning of the users, navigate to **Tools > Task Management** on Cisco Unity Connection Administration (CUCA) and schedule **Branch Provisioning Synchronization Task**. For more information on scheduling a task, refer to the "Cisco Unity Connection 10.x Tool Settings" chapter of *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

By default, a maximum of 5 provisioning threads can run at a particular instant of time. However, you can also change this value to a desired number. To change the number of provisioning threads that can run simultaneously, you need to perform the following steps on command prompt of central Unity Connection server using administrator credentials:

**Step 1** Run the following command:

```
run cuc dbquery unitydirdb EXECUTE PROCEDURE
csp_ConfigurationModify(pFullName='System.SRSV.MaxProvisioningThreads', pValue='<any_value
< 50 >');
```

For example, if you want to run 15 provisioning threads simultaneously, run the following command:

```
run cuc dbquery unitydirdb EXECUTE PROCEDURE
csp_ConfigurationModify(pFullName='System.SRSV.MaxProvisioningThreads', pValue='15');
```

**Step 2** Run the following command to confirm that the value of "System.SRSV.MaxProvisioningThreads" field is set to 15:

```
run cuc dbquery unitydirdb select objectid,fullname,value from vw_configuration
where fullname like '%SRSV%'
```

After changing the value of System.SRSV.MaxProvisioningThreads to 1, you need to restart the **Unity Connection Branch Sync Service** and **Tomcat Service** to reflect the changes.

You can use either of the following methods to upload voicemails from the branch system to the central Unity Connection server:

- **Manual Synchronization of Voicemail Messages**: To manually upload voicemails from the branch to the central Unity Connection server, navigate to **Branch Management > Edit Branch** on Cisco Unity Connection Administration (CUCA) and select **Voicemail Upload**.

- **Automatic Synchronization of Voicemail Messages**: To automatically enable the uploading of voice messages from the branch to the central Unity Connection server, navigate to **Tools > Task Management** on Cisco Unity Connection Administration (CUCA) and schedule **Branch Voice mail polling task**. For more information on scheduling a task, refer to the "Cisco Unity Connection 10.x Tool Settings" chapter of *Interface Reference Guide for Cisco Unity Connection Administration Release 10.x* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/gui_reference/guide/10xcucgrgx.html.

# Configuring an SRSV User

You can either create a new user or update an existing user to provide access to the SRSV feature. Before creating an SRSV user, make sure that all the required services, such as Unity Connection REST Service and Unity Connection Branch Sync Service are started on the central Unity Connection server and on the branch. For more information on services required for SRSV feature, refer to the *Administration Guide for Cisco Unity Connection Serviceability Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/serv_administration/guide/10xcucservagx.html.

## Task List to create an Unity Connection SRSV User

To create an Unity Connection SRSV user, you need to perform the following tasks:

**Step 1** *Creating a Partition*: Create a partition on the Unity Connection server. For more information on how to create a partition, refer to the "Managing Partitions in Cisco Unity Connection 10.x" section of the "Managing Partitions and Search Spaces in Cisco Unity Connection 10.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 10.x* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx.html.

**Step 2** *Creating a Branch*: Create a branch on the Unity Connection server with details of the Cisco Unity Connection SRSV server, which corresponds to the partition created above. For more information on how to create a branch, refer to the Managing Branches in Cisco Unity Connection 10.x, page 47-6 section.

**Step 3** *Creating a New User or Assigning the Partition to an Existing User*: Assign the partition created above to an existing user or create a new user and assign the partition to the user for providing access to the SRSV feature. For more information on how to create a user, refer to the "Creating Cisco Unity Connection 10.x User Accounts in Cisco Unity Connection Administration" section of the "Adding Cisco Unity Connection 10.x Accounts Individually" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 10.x* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/user_mac/guide/10xcucmacx.html.

# Managing Branches in Cisco Unity Connection 10.x

You can create a branch in Cisco Unity Connection Administration, which is further associated with a partition of users having access to SRSV functionality.

### To Create a Branch

**Step 1** In Cisco Unity Connection Administration, expand **Networking** > **Branch Management**, then select **Branches**.

**Step 2** On the **Branch Listing** page, select **Add New**.

**Step 3** On the **New Branch** page, enter basic settings, as applicable. (For field information, on the **Help** menu, select **This Page**.)

**Note** Fields marked with * (an asterisk) are required.

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

**Step 5** On the **Edit Branch** page, continue entering applicable settings.

**Step 6** When you have finished entering settings on the **Edit Branch** page, select **Save**.

# Shortcut Keys for Cisco Unity Connection Administration

Following are the details on the usage of shortcut keys for Cisco Unity Connection Administration:

- The administrator can use the TAB key to navigate all links, all form fields, and widgets in the sequential order. After login, when the administrator first presses the TAB key then focus comes on top of the tree labeled as "Cisco Unity Connection". Then by pressing the TAB key again, the administrator can traverse all links, all form fields, and widgets.
- At any time if the administrator wants to navigate the pages corresponds to the tree link, then press the 'ENTER' key after selecting the link using the TAB key.
- Once focus goes to page frame then by pressing TAB key you can traverse all visual adds on that page.
- The administrator can move the focus from any of the page/form to the top of the tree by the "Ctrl+Alt+t" key. This shortcut key will focus the top tree label "Cisco Unity Connection" and from there you can traverse all tree links using the TAB key.
- The Ctrl+Alt+t shortcut can be used at anywhere on tree and pages to focus tree label "Cisco Unity Connection".
- These shortcut keys work on Windows and MAC operating system.

| Item | Internet Explorer | Mozilla Firefox | Safari/Chrome | Usage |
|---|---|---|---|---|
| Forward navigation of links, form fields, and widget on Connection Administration | TAB | TAB<br>Note: The TAB key does not work on MAC for any hyperlink navigation. To make it work, the administrator needs to do some configuration changes in Firefox that is explained below. | TAB | The TAB key is used to navigate all links, all form fields, and widget in the forward sequence.<br>To select or unselect radio button we can use any Arrow key. |
| Focus on the top of Connection Administration tree | Ctrl+Alt+t | Ctrl+Alt+t | Ctrl+Alt+t | This shortcut key is used to bring focus back on the top of tree in the Connection Administration page. |
| Backward navigation of links, form fields, and widget on Connection Administration | Shift+TAB | Shift+TAB | Shift+TAB | This combination of key is used to navigate links, form fields, and widget in the backward sequence. |
| Navigate menu item | Left or Right arrow key | Left or Right arrow key | Left or Right arrow key | First bring focus on any menu item using TAB or Shift+TAB, then use the Left or Right arrow key for navigation for all menu items |

| Item | Internet Explorer | Mozilla Firefox | Safari/Chrome | Usage |
|---|---|---|---|---|
| Navigate drop down list Item | Up or Down arrow key | Up or Down arrow key | Up or Down arrow key | First bring focus on the dropdown list using TAB or Shift+TAB then use Up or Down arrow key to navigate all list item. |
| Expand and Collapse tree on Connection Administration | ENTER Key | ENTER Key | ENTER Key | First bring focus on tree node then press ENTER to expand and collapse the tree for fast navigation |

#### To enable TAB Key navigation for hyperlink on Safari

The TAB key does not work on the Safari browser for hyperlink navigation. Therefore, left most tree is not accessible on the Connection Administration page through the TAB key directly. To make the tree accessible through TAB key it is required to change the following browser settings on Safari.

**Step 1** Click goto **Preferences>Advanced.**

**Step 2** Select the Press tab to highlight each item on a web page checkbox to make the tree links accessible using the TAB key.

#### To enable TAB Key navigation for hyperlink on MAC

**Step 1** Open the Firefox browser and type about:config in the address bar.

**Step 2** Press 'ENTER' key.

**Step 3** Accept the security warning.

**Step 4** There will be a list of configuration parameters. Try to search for "accessibility.tabfocus".

**Step 5** If it is not there in the list then add this parameter as an "integer" and give its value "7".

**Step 6** Refresh the page and use TAB key for page navigation.

**Note** If there is a DTMF number in the display name then the part of the name after DTMF digit will not play as recorded name.

# Other Unity Connection Features

Other Unity Connection Features that can improve the Accessibility for the end user:

- Speech Connect for Cisco Unity Connection
- Cisco SpeechView
- TTY Overview

# Speech Connect for Cisco Unity Connection

Cisco Unity Connection includes a speech-enabled enhancement to the automated attendant functionality, called Speech Connect. Speech Connect uses voice-enabled directory handlers that allow both employees and outside callers can say the name of an employee and instantly be connected, without having to navigate an audio-text tree, and without knowing the extension of the employee. For easy access for employees, you can configure a Speech Connect speed dial on user phones.

If multiple employees have the same name or if Speech Connect does not have a perfect match for the name spoken by the caller, it presents numerous name choices for the caller and can include additional information such as the employee location or department. Speech Connect also plays the recorded name of the employee in his or her own voice, if available, making it easier for the caller to choose among multiple names.

For detailed information about setting up directory handlers, see the "Managing Directory Handlers in Cisco Unity Connection 10.x" chapter of the System Administration Guide for Cisco Unity Connection Release 10.x, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx.html.

For more information on Speech Connect, see the http://www.cisco.com/en/US/products/ps10670/index.html.

# Cisco SpeechView

SpeechView feature allows you to receive voice messages in your mail box in the form of text. When a voice message arrives, it is delivered to the mailbox of the recipient with a blank text attachment. When the completed transcription is returned by the transcription service, the text attachment is updated with the text of the transcription or with an error message if there was a problem with the transcription. Only the first 500 characters of a message transcription are provided, so longer messages are truncated. However, users have access to the original recording in its entirety.

SpeechView is a feature of the Connection unified messaging solution; therefore, the original audio version of each voice message remains available to you anywhere, anytime.

For more information on SpeechView, see the http://www.cisco.com/en/US/products/ps10671/index.html.

# TTY Overview

A TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call in to Unity Connection and use the same features that a hearing caller can use. However, note the following limitations:

- G.711 MuLaw must be selected as the message recording and storage codec. The Unity Connection TTY prompt set is not compatible with G.729a or other message recording and storage codecs.
- A dedicated phone number must be set up for use by outside callers with TTY. All greetings, prompts, and subscriber names accessible from this number must be created with the TTY prompt set.
- TTY is a TUI language only. At the present time, there is no compatible Text to Speech (TTS) language for TTY. The TTY prompt set is also not suitable for use as a GUI language.
- TTY tones are not available for use in navigating through the Unity Connection conversation. Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.
- Due to recording and playback limitations, the TTY prompt set cannot be used in interview handlers.
- TTY phones do not display the voice names but simply playback the voice names.
- Use TTY angel to display voice name as text and replace them in Unity Connection.

For more information on TTY feature, see the http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsag060.html#wp1097525.

## A


abbreviated extensions 6-10

accounts

- Operator 22-7
- UndeliverableMessagesMailbox 22-7
- Unity Connection Messaging System 22-8

adding

- alternate names for a system distribution list 30-5
- AXL servers 32-5
- Cisco Unified Communications Manager servers 32-11
- description of message attachments 40-1
- global nicknames to list 16-22
- integration, phone system 32-2
- members to system distribution lists 30-4
- PIMG/TIMG units 32-16
- port 32-18
- port group 32-8
- SIP server 32-14
- system distribution lists 30-2
- TFTP server 32-13

All Hours schedule 12-1

All Voicemail Users distribution list 30-1

alternate contact numbers, configuring for call handlers 6-9

alternate conversations

- Optional Conversation 1 15-3
- overview 15-3

alternate names, adding for system distribution lists 30-5

application plug-ins 3-2

Attempt Forward call routing rule 10-1

Attempt Sign-In call routing rule 10-1

audio format

- changing for calls 18-1, 19-1, 32-9, 32-10
- changing for recordings 18-2, 19-2, 20-5, 22-5

authentication, configuring LDAP 44-8

authentication rules

- default rules 21-2
- overview 21-2

automated attendant 4-9

AXL servers

- adding 32-5
- changing settings 32-7
- deleting 32-7


## B


backing up and restoring data 3-7

backup and restore application for migrations (COBRAS) 3-2

Broadcast Message Administrator

- setting up access 29-2
- using 29-6

broadcast messages

- changing default settings 29-7
- overview 29-1
- setting up access for sending 29-2

Bulk Administration Tool, accessing 3-3


## C


calendar integration

- about 36-1
- creating with Cisco Unified MeetingPlace 36-16
- creating with Cisco Unified MeetingPlace Express 36-21
- creating with Exchange 2003 36-9

creating with Exchange 2007 36-2

Exchange contacts 36-1

caller input settings, changing user sign-in settings 16-17

caller options, user settings 15-6

call handlers

caller input and one-key dialing 6-9

call transfer settings 6-13

default 6-1

deleting 6-13

Goodbye 6-2

greetings 6-6

modifying 6-5

Opening Greeting 6-1

Operator 6-2

overview 4-2

Route From Next Call Routing Rule Action, using with routing rules 4-6

taking messages 6-12

templates, modifying 6-3, 6-4

call handler templates

creating 6-2

default templates 6-2

deleting 6-2

modifying 6-2

Call Handler Traffic report, description 43-4

call holding, user settings in Connection Messaging Assistant 15-5

call loop detection 32-5

call management

creating a map 5-1

implementing a plan 5-2

managing call handlers 6-1

managing call routing tables 10-1

managing directory handlers 7-1

managing interview handlers 8-1

managing restriction tables 13-1

managing schedules and holidays 11-1, 12-1, 35-1

overview 4-1

planning 5-1

call routing tables

adding rules 10-2

and the Route From Next Call Routing Rule action 4-6

Attempt Forward rule 10-1

Attempt Sign-In rule 10-1

changing the order of rules 10-3

default rules 10-1

deleting rules 10-4

modifying rules 10-2

Opening Greeting rule 10-1

overview 4-4

calls, changing the audio format (or codec) for 18-1, 19-1, 32-9, 32-10

call screening, user settings in Connection Messaging Assistant 15-5

call transfers

user settings in Connection conversation 15-6

user settings in Connection Messaging Assistant 15-6

call waiting, configuring hold time 16-5

capacity of hard disk, specifying maximum percentage 22-19

certificate, viewing for port 32-21

changing

addressing and recording order 16-2, 16-3

addressing priority lists, how names are stored in 16-2

AXL server settings 32-7

call loop detection settings 32-5

Cisco Unified Communications Manager server settings 32-12

codec preference settings 32-9

description of message attachments 40-2

dial prefix settings for live reply to unidentified callers 16-12

message deletion options 16-12, 16-14

message skipping during playback (Optional Conversation 1) 16-19

MWI settings 32-11

normalization setting 32-17

phone system settings 32-3

- phone system trunk settings 32-23
- PIMG/TIMG settings 32-16
- port group advanced settings 32-17
- port group settings 32-9
- port settings 32-19
- SIP server settings 32-15
- SIP settings 32-17
- system prompt language 16-13
- TFTP server settings 32-14
- user sign-in settings during user greeting 16-17

Cisco DirSync service, activating 44-4

Cisco Fax Server integration
- about 34-1
- changing the Cisco Unity Connection configuration 34-8
- changing the user configuration 34-9
- configuring Cisco Unity Connection 34-6
- configuring single number for calls and faxes 34-9
- configuring the Cisco Fax Server 34-2
- configuring users 34-7
- creating 34-1
- requirements 34-2
- testing 34-7

Cisco PCA, securing access to Cisco Unity Connection 28-1

Cisco SIP Proxy Server
- adding 32-14
- changing settings 32-15
- deleting 32-15

Cisco Unified Communications Manager
- adding servers 32-11
- adding TFTP server 32-13
- AXL servers, adding 32-5
- AXL servers, deleting 32-7
- changing AXL server settings 32-7
- changing server settings 32-12
- changing TFTP server settings 32-14
- deleting servers 32-12
- deleting TFTP server 32-13
- port certificate 32-21
- root certificate for Connection 32-24

Cisco Unified MeetingPlace, creating a calendar integration 36-16

Cisco Unified MeetingPlace Express, creating a calendar integration 36-21

Cisco Unified Mobility Advantage integration
- about 33-1
- configuring Cisco Unity Connection 33-2
- requirements 33-2
- task list for creating 33-1
- testing 33-3

Cisco Unified Real-Time Monitoring Tool (RTMT) 3-8

Cisco Unified Serviceability 3-8

Cisco Unified Serviceability services
- configuring enterprise parameters 38-1
- configuring service parameters 37-1
- descriptions of enterprise parameters 38-2
- descriptions of service parameters 37-2

Cisco Unity Connection Administration
- accessing 2-1
- configuring browsers 1-1
- finding records 2-3
- interface 2-2
- using Help 2-3

Cisco Unity Connection conversation 15-1

Cisco Unity Greetings Administrator
- overview 20-2
- setting up 20-4
- using 20-3

Cisco Utilities Database Link for Informix 3-10

Cisco Voicemail Organization 1-1

Cisco Voice Technology Group Subscription tool 3-8

COBRAS backup and restore application 3-2

codec
- changing for calls 18-1, 19-1, 32-9, 32-10
- changing for recordings 18-2, 19-2, 20-5, 22-5
- changing preference settings 32-9
- effect on recording time available and disk space used 26-1

Connection 1.x, migrating from 3-2
Connection Administration, accessing 3-2
Connection Serviceability 3-6
Connection User Data Dump 3-10
contact integration
about 36-2
creating with Exchange 2003 36-9
creating with Exchange 2007 36-2
Exchange contacts 36-2
contacts, user settings in Connection Messaging Assistant 15-8
conversation
allowing voice recognition users to say their voicemail PINs 16-20
alternate conversation versions 15-3
caller options 15-1
changing addressing and recording order 16-2, 16-3
changing dial prefix settings for live reply to unidentified callers 16-12
changing how names are stored in user addressing priority lists 16-2
changing message deletion options 16-12, 16-14
changing PIN re-entry behavior 16-18
Cisco Unity Connection, overview 15-1
customizing by administrators 15-2
customizing by users 15-5
documenting for users 3-10
easy sign-in 16-18
sign-in 16-17
specifying caller information before message playback 16-11
user options 15-1
user settings in Connection conversation 15-6
user settings in Connection Messaging Assistant 15-6
using voice commands 15-4
creating
AXL servers 32-5
call handler templates 6-2
call management map 5-1
call routing rules 10-2
directory handlers 7-2, 9-2
holiday schedules 11-9, 12-1, 35-2
interview handlers 8-1
restriction tables 13-2
schedules 12-2, 35-2, 35-4
user accounts 1-1
credentials policies 21-1
CUDLI 3-10
Custom Keypad Mapping tool
accessing 17-2
conversations that can be customized 17-3
documenting keymap for users 17-13
guidelines 17-2
resetting 17-2
using 17-1

## D

Database Proxy 3-9
deleting
AXL servers 32-7
call handlers 6-13, 7-5, 9-5
call handler templates 6-2
call routing rules 10-4
Cisco Unified Communications Manager servers 32-12
description of message attachments 40-2
integration, phone system 32-2
interview handlers 8-4
members from system distribution lists 30-4
phone system trunk 32-22
PIMG/TIMG units 32-16
port 32-19
port group 32-8
restriction tables 13-3
schedules 12-3, 35-4
SIP server 32-15
TFTP server 32-13
Dial Plan report, description 43-2

Dial Search Scope report, description 43-2
Digital Networking 1-1
directory handlers
creating 7-2, 9-2
default 7-1, 9-1
deleting 7-5, 9-5
modifying 7-2, 9-2
overview 4-3
System Directory Handler 7-1, 9-1
Disaster Recovery System 3-7
disk space used, effect of codec on 26-1
dispatch messages 22-8
Distribution Lists report, description 43-3

## E

easy sign-in conversation 16-18
Edit Disk Capacity Configuration page 22-19
email
configuring text-to-speech access to Exchange 42-1
messages 22-2
enabling
Text to Speech for a user 11-5, 11-6
end of recording, configuring termination warning prompt 22-6
enterprise parameters
configuring for Cisco Unified Serviceability services 38-1
descriptions 38-2
for Cisco Unified Serviceability services 38-1
Exchange
configuring text-to-speech access to email 42-1
configuring text-to-speech access to Exchange 2003 emails 42-6
configuring text-to-speech access to Exchange 2007 emails 42-1
Exchange 2003, creating a calendar and contact integration 36-9
Exchange 2007, creating a calendar and contact integration 36-2
Exchange contacts
enabling importing from Exchange 2003 36-9
enabling importing from Exchange 2007 36-2
extensions
adding prepended digits 6-10
converting LDAP phone numbers into (Connection 8.5) 44-5
external message store, configuring access to emails in 42-1

## F

fax
about the Cisco Fax Server integration 34-1
changing the Cisco Unity Connection configuration 34-8
changing the user configuration 34-9
configuring Cisco Unity Connection 34-6
configuring single number for calls and faxes 34-9
configuring the Cisco Fax Server 34-2
configuring users 34-7
creating a Cisco Fax Server integration 34-1
requirements for the Cisco Fax Server integration 34-2
testing 34-7
field definitions 2-3
Firefox, configuring 1-1

## G

G.711 A-Law codec
selecting for calls 18-1, 19-1, 32-9, 32-10
selecting for recordings 18-2, 19-2, 20-5, 22-5
G.711 Mu-Law codec
selecting for calls 18-1, 19-1, 32-9, 32-10
selecting for recordings 18-2, 19-2, 20-5, 22-5
G.729a codec
selecting for calls 18-1, 19-1, 32-9, 32-10
selecting for recordings 18-2, 19-2, 20-5, 22-5
G726 codec, selecting for recordings 18-2, 19-2, 20-5, 22-5

global nicknames
adding names to list 16-22
editing list 16-22
Goodbye call handler 6-2
Grammar Statistics tool, accessing 3-4
greetings
call handlers 6-6
changing audio format for recording 20-5
recording by using Media Master 20-1
user settings in Connection conversation 15-6
user settings in Connection Messaging Assistant 15-6
groupware email messages 22-2

## H

hard disk, specifying maximum capacity 22-19
Help
page and field 2-3
using 2-3
holidays
designating 11-9, 12-1, 35-2
holiday schedule 12-1

## I

identified user messaging 22-2
IMAP access
accessing email messages from Connection by using 22-2
configuration procedures 23-5, 24-5
configuration task list 23-3
Connection server configuration 23-6
security recommendations 23-3
SMTP message parameters 23-7
IMAP clients
integrated messaging example 23-2
securing access to Cisco Unity Connection 28-1
SMTP message handling 23-1
Import Users tool, accessing 3-4
integrated messaging, example 23-2
integration
adding 32-2
adding phone system trunk 32-22
adding PIMG/TIMG units 32-16
adding port 32-18
adding port group 32-8
adding SIP certificate 32-25
adding SIP security profile 32-26
adding SIP server 32-14
adding TFTP server 32-13
AXL server, changing settings 32-7
AXL servers, adding 32-5
AXL servers, deleting 32-7
call loop detection, changing settings 32-5
changing Cisco Unified Communications Manager server settings 32-12
changing phone system trunk settings 32-23
changing PIMG/TIMG settings 32-16
changing port group advanced settings 32-17
changing port settings 32-19
changing SIP certificate 32-26, 32-27
changing SIP server settings 32-15
changing SIP settings 32-17
changing TFTP server settings 32-14
codec, changing preference settings 32-9
deleting 32-2
deleting Cisco Unified Communications Manager servers 32-12
deleting phone system trunk 32-22
deleting PIMG/TIMG units 32-16
deleting port 32-19
deleting SIP certificate 32-25
deleting SIP security profile 32-26
deleting SIP server 32-15
deleting TFTP server 32-13
enabling or disabling normalization 32-17
IPv6 32-27
MWI, disabling the use of the same port for turning on and off 32-4

MWI, synchronizing 32-4
MWIs, changing settings 32-11
phone system, changing settings 32-3
phone system trunk description 32-22
port certificate 32-21
port description 32-18
port group, changing settings 32-9
port group, deleting 32-8
port group description 32-7
root certificate for Connection 32-24
security for ports 32-23
users associated with phone system 32-3
viewing root certificate for Connection 32-24
Internet Explorer, configuring 1-2
internetworking Cisco Unity Connection servers 1-1
interview handlers
creating 8-1
deleting 8-4
modifying 8-2
overview 4-3
intrasite or intersite links 1-1
IPv6 32-27


## L


language
changing system prompt language 16-13
language settings for call handlers 6-12
language settings for directory handlers 7-3
language settings for interview handlers 8-3
language settings for routing rules 10-3
message subject line format 22-16
LDAP
activating the Cisco DirSync service 44-4
adding configurations and synchronizing data 44-14
changing LDAP directory configurations 44-15
configuring authentication 44-8
converting LDAP phone numbers into Connection extensions (Connection 8.5) 44-5
deleting LDAP directory configurations 44-16
disabling authentication 44-9
enabling synchronization 44-4
task list for configuring 44-2
license files
about using MAC addresses on physical servers 45-2
live record
about 22-5
configuring 22-22
lockout policy 21-1


## M


mailboxes, moving 25-5
mailbox size quotas, setting systemwide and mailbox-store limits 26-1
Mailbox Store report, description 43-2
mailbox stores
backing up 25-3
creating 25-4
deleting 25-6
disabling 25-7
maximum size 25-3
maximum size, changing 25-6
message handling when maximum size is exceeded 22-13
moving mailboxes 25-5
multiple 25-1
Maximum Delay for TTS Access Before Timeout 22-11
Media Master, recording greetings and names 20-1
MeetingPlace, creating a calendar integration 36-16
MeetingPlace Express, creating a calendar integration 36-21
message actions, configuring 22-15
message addressing
user settings in Connection conversation 15-7
user settings in Connection Messaging Assistant 15-7
message aging 26-4
message aging alerts

about 26-4, 26-5
configuration procedures 26-7, 26-8
message attachment
adding 40-1
changing 40-2
deleting 40-2
message locator, phone view 41-1
message notification
setting up, SMS (SMPP) 27-2
user settings in Connection conversation 15-7
user settings in Connection Messaging Assistant 15-7
message playback
user settings in Connection conversation 15-7
user settings in Connection Messaging Assistant 15-7
message recording expiration 26-9
messages
actions, configuring 22-15
aging 26-4
aging alerts 26-4, 26-5
dispatch messages 22-8
expiration 26-9
groupware email messages 22-2
how Connection handles messages that are interrupted by disconnected calls 22-12
how Connection handles messages that cannot be delivered 22-11
how Connection handles messages when mailbox quotas are exceeded 22-13
how Connection handles messages when maximum mailbox store size is exceeded 22-13
how Connection handles messages when system components are unavailable 22-11
interview messages 22-5
live record 22-5
message delivery 22-10
message storage 22-19
migrating from Connection 1.x 3-5
migrating from Connection 1.x using COBRAS (recommended) 3-2
migrating from Unity 3-5
migrating from Unity using COBRAS (recommended) 3-2
notifications 22-3
outside caller voice messages 22-1
receipts 22-4
sensitivity 22-14
shredding files for secure deletes 22-21
subject line format 22-16
system broadcast messages 22-2
types of messages 22-1
user to user voice messages 22-2
Message Traffic report, description 43-2
message waiting indicators, synchronizing for phone system 32-4
messaging overview 22-1
Migrate Messages utility, accessing 3-5
Migrate Users utility, accessing 3-6
migrating data and messages from Unity or Connection 1.x 3-2
modifying
call handlers 6-5
call handler templates 6-2, 6-3, 6-4
call routing rules 10-2
directory handlers 7-2, 9-2
interview handlers 8-2
restriction tables 13-3
schedules 12-2, 35-3
system distribution lists 30-3, 30-5
multiple mailbox stores 25-1
MWIs
changing settings 32-11
disabling the use of the same port for turning on and off 32-4
synchronizing for phone system 32-4


## N


names, recording by using Media Master 20-1
networking 1-1
normalization, enabling or disabling for port group 32-17

notification
setting up, SMS (SMPP) 27-2
user settings in Connection conversation 15-7
user settings in Connection Messaging Assistant 15-7

## O

one-key dialing
configuring 6-9
overview 6-9
Opening Greeting
call handler 6-1
call routing rule 10-1
Operator call handler 6-2
Operator user 22-7
Optional Conversation 1
changing message skipping behavior 16-19
overview 15-3
Outcall Billing Detail report, description 43-4
Outcall Billing Summary report, description 43-4
outside caller voice messages 22-1

## P

page Help 2-3
partitions
changing default 31-11
creating 31-9
default 31-3
deleting 31-9
finding objects in 31-11
modifying 31-9
overview 31-1
password policy 21-1
PCM codec, selecting for recordings 18-2, 19-2, 20-5
personal call transfer rules, integration with Exchange contacts 36-2
personal settings
user settings in Connection conversation 15-8
user settings in Connection Messaging Assistant 15-8
Phone Interface Failed Sign-In report, description 43-1
phone language, changing 16-13
phone system
adding AXL servers 32-5
adding integration 32-2
changing AXL server settings 32-7
changing settings 32-3
deleting AXL servers 32-7
deleting integration 32-2
disabling the use of the same port for turning on and off an MWI 32-4
list of users associated with 32-3
synchronizing MWIs 32-4
phone system trunk
changing settings 32-23
deleting 32-22
description 32-22
Phone View 32-4, 41-1
PIMG unit
adding 32-16
changing settings 32-16
deleting 32-16
PIN policy 21-1
plugins
application 3-2
installing 39-1
overview 39-1
Port Activity report, description 43-2
port group
adding 32-8
changing advanced settings 32-17
changing settings 32-9
deleting 32-8
description 32-7
enabling or disabling normalization 32-17
port memory, disabling 32-4
ports
adding 32-18

adding SIP certificate 32-25
adding SIP security profile 32-26
changing settings 32-19
changing SIP certificate 32-26, 32-27
deleting 32-19
deleting SIP certificate 32-25
deleting SIP security profile 32-26
description 32-18
port certificate for Connection 32-21
root certificate for Connection 32-24
security 32-23
viewing root certificate for Connection 32-24
prepended digits for extensions 6-10
private lists
user settings in Connection conversation 15-8
user settings in Connection Messaging Assistant 15-8
prompts
overview 15-2
what you can change 15-2


## Q


quotas, message handling when exceeded 22-13


## R


recordings
changing the audio format (or codec) for 18-2, 19-2, 20-5, 22-5
configuring termination warning prompt 22-6
greetings and names 20-1
selecting device 20-2
recording time available, effect of codec on 26-1
relay settings for private and secure messages 23-5
Remote Administration Tools 3-9
reports
archiving data 43-5
configuration parameters 43-4
generating and viewing 43-5
overview 43-1
restriction tables
creating 13-2
default 13-1
Default Fax 13-1
Default Outdial 13-1
Default System Transfer 13-1
Default Transfer 13-1
deleting 13-3
modifying 13-3
overview 4-6
root certificate
saving as file 32-24
viewing 32-24
Route From Next Call Routing Rule action 4-6
RSS Feeds 22-24


## S


sag-03-01 3-1
sag-03-02 3-2
sag-03-03 3-2
sag-03-04 3-2
sag-03-05 3-3
sag-03-06 3-3
schedules and holidays
All Hours 12-1, 35-1
creating schedules 12-2, 35-2, 35-4
default 12-1
deleting schedules 12-3, 35-4
designating holidays 11-9, 12-1, 35-2
Holidays 12-1, 35-1
modifying schedules 12-2, 35-3
overview 4-8
Voice Recognition Update 12-1, 35-1
Weekdays 12-1, 35-1
search spaces
and call handlers 31-7
and call routing rules 31-6

and contacts 31-8
and digital networking 31-8
and directory handlers 31-7
and interview handlers 31-7
and system distribution lists 31-7
and user objects 31-5
and VPIM locations 31-8
changing default 31-11
creating 31-10
default 31-3
deleting 31-10
example configurations 31-3
finding objects in 31-11
modifying 31-10
overview 31-2
secure deletes, shredding message files for 22-21
securing Cisco PCA and IMAP client access to Cisco Unity Connection 28-1
security
adding SIP certificate 32-25
adding SIP security profile 32-26
changing SIP certificate 32-26, 32-27
deleting SIP certificate 32-25
deleting SIP security profile 32-26
description for ports 32-23
policies 21-1
port certificate 32-21
relay settings for private and secure messages 23-5
root certificate for Connection 32-24
viewing root certificate for Connection 32-24
service parameters
configuring for Cisco Unified Serviceability services 37-1
descriptions 37-2
for Cisco Unified Serviceability services 37-1
Session Initiation Protocol (SIP), changing settings 32-17
session timeout setting, Cisco Unity Connection Administration 2-1
setting up
SMS (SMPP) message notifications 27-2
Show Dependency Results 3-7
shredding message files for secure deletes 22-21
sign-in conversation 16-17
sign-in policy 21-1
simulating abbreviated extensions 6-10
SIP
adding SIP certificate 32-25
adding SIP security profile 32-26
changing SIP certificate 32-26, 32-27
deleting SIP certificate 32-25
deleting SIP security profile 32-26
SIP server
adding 32-14
changing settings 32-15
deleting 32-15
SMS (SMPP) message notifications, setting up 27-2
SMTP
messages, overview 23-1
speech to text 24-1
SpeechView
configuring 24-1
SpeechView Activity Report by User, description 43-4
SpeechView Activity Summary Report, description 43-4
SSL certificate, using to secure Cisco PCA and IMAP client access to Cisco Unity Connection 28-1
Subscriber Information Dump. See Connection User Data Dump.
synchronizing MWIs for phone system 32-4
Synch Users Tool, accessing 3-4
System Configuration report, description 43-4
System Directory Handler 7-1, 9-1
system distribution lists
adding alternate names 30-5
adding and removing members 30-4
creating 30-2
default lists 30-1
modifying 30-3, 30-5
overview 30-1
system prompts

changing language 16-13
customizing 15-2
system transfers, setting up 14-1


## T


Task Management tool, accessing 3-7
termination warning prompt, configuring 22-6
Text Notifications 22-3
text to speech
about 42-1
configuring access to Exchange 2003 emails 42-6
configuring access to Exchange 2007 emails 42-1
Text to Speech, enabling for a user 11-5, 11-6
TFTP server
adding 32-13
changing settings 32-14
deleting 32-13
timeouts in Cisco Unity Connection Administration 2-1
TIMG unit
adding 32-16
changing settings 32-16
deleting 32-16
tools, Custom Keypad Mapping 17-1
transcriptions 24-1
Transfer Call Billing report, description 43-3
trunk, phone system
adding 32-22
changing settings 32-23
deleting 32-22


## U


Undeliverable Messages distribution list 30-2
UndeliverableMessagesMailbox user 22-7
unidentified caller messages 22-1
Unity, migrating from 3-2
Unity Connection Messaging System user 22-8
Unused Voice Mail Accounts report, description 43-3
user accounts, creating 1-1
User Lockout report, description 43-3
User Message Activity report, description 43-3
User Phone Sign-In and MWI report, description 43-3
users
list of users associated with phone system 32-3
migrating from Connection 1.x 3-6
migrating from Connection 1.x using COBRAS (recommended) 3-2
migrating from Unity 3-6
migrating from Unity using COBRAS (recommended) 3-2
Operator 22-7
UndeliverableMessagesMailbox 22-7
Unity Connection Messaging System 22-8
user speech recognition conversation 15-4
Users report, description 43-1
user to user voice messages 22-2
user workstations, setting up 1-1
utilities and tools
Bulk Administration Tool 3-3
Cisco Unified Serviceability 3-8
Cisco Voice Technology Group Subscription Tool 3-8
Connection Administration 3-2
Connection Serviceability 3-6
Disaster Recovery System 3-7
Grammar Statistics 3-4
Import Users 3-4
Migrate Messages 3-5
Migrate Users 3-6
plug-ins 3-2
RTMT 3-8
Synch Users 3-4
Task Management 3-7

## V

ViewMail for Microsoft Outlook, integrated messaging example 23-2
voice commands, using 15-4
voice commands, using to call Exchange contacts 36-2
voice messages
  delivery 22-10
  dispatch messages 22-8
  interviews 22-5
  live record 22-5
  notifications 22-3
  outside caller 22-1
  receipts 22-4
  system broadcast 22-2
  user to user 22-2
voice messaging port
  adding 32-18
  changing settings 32-19
  deleting 32-19
voice recognition
  allowing users to say their voicemail PINs 16-20
  Grammar Statistics tool 3-4
Voice Recognition Update schedule 12-1
voice to text 24-1
VPIM networking 1-1

## W

Wallet Card Wizard 3-10
warning prompt for end of recording, configuring 22-6
Weekdays schedule 12-1